Werk

Titel: Konstruktion aller Automorphismen der Ordnung 2 einer endlichen elementaren abels...

Autor: LATT, K.

Jahr: 1980

PURL: https://resolver.sub.uni-goettingen.de/purl?301416052_0010|log15

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Beiträge zur Algebra und Geometrie
10 (1980), 111 – 140

Konstruktion aller Automorphismen der Ordnung 2 einer endlichen elementaren abelschen Gruppe

Klaus Latt

Einleitung

Es sei A eine beliebige endliche abelsche Gruppe. Ein Automorphismus σ der Ordnung 2 von A ist dann dadurch gekennzeichnet, daß für ihn $\sigma(\sigma(a)) = a$ für alle $a \in A$ gilt. Ziel der Arbeit ist es, für den Spezialfall einer endlichen elementaren abelschen Gruppe G konstruktive Verfahren zur Gewinnung aller Automorphismen der Ordnung 2 aufzustellen und ihre Anzahl zu bestimmen.
Eine endliche elementare abelsche Gruppe G ist eine endliche abelsche p-Gruppe vom Typus $(p, p, \ldots, p)$, wobei p eine Primzahl bedeutet (siehe auch [4], S. 105). Hat G den Rang n [= Anzahl der Elemente einer Basis von G = Anzahl der p's in der Typusbezeichnung $(p, p, \ldots, p)$ von G, wobei stets $n \geqq 1$, also G immer als $\neq \{0\}$ angenommen wird] und ist σ ein Automorphismus der Ordnung 2 von G, so gilt für eine feste Basis $a_1, \ldots, a_n$ von G

$$\begin{pmatrix} \sigma(a_1) \\ \vdots \\ \sigma(a_n) \end{pmatrix} = \begin{pmatrix} \alpha_{11} \ldots \alpha_{1n} \\ \vdots \quad\quad \vdots \\ \alpha_{n1} \ldots \alpha_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \tag{1}$$

wobei die α_{ik} nichtnegative ganze Zahlen mod p darstellen und für die (n-reihige) Matrix $\mathfrak{A}_n = (\alpha_{ik})$ der α_{ik} die Kongruenz

$$\mathfrak{A}_n^2 \equiv \mathfrak{E} \bmod p \quad (\mathfrak{E}_n \text{ Einheitsmatrix}) \tag{2}$$

gilt. Ein Automorphismus σ der Ordnung von G bestimmt also durch (1) eindeutig eine Matrix $\mathfrak{A}_n$, deren Elemente α_{ik} mod p reduzierte nichtnegative ganze Zahlen sind und von der (2) erfüllt wird. Genügt umgekehrt eine Matrix $\mathfrak{A}_n$, deren Elemente α_{ik} mod p reduzierte nichtnegative ganze Zahlen sind, der Bedingung (2), so wird eindeutig durch (1) ein Automorphismus σ der Ordnung 2 von G festgelegt.
Lassen sich also alle Automorphismen σ der Ordnung 2 einer endlichen elementaren abelschen Gruppe G vom Rang n für die Primzahl p konstruieren, so erhält man damit auch alle Lösungen der Matrizenkongruenz

$$\mathfrak{X}_n^2 \equiv \mathfrak{E}_n \bmod p. \tag{3}$$

Entsprechend liefert eine Formel für die Anzahl $\mathrm{Aut}_2(G, p)$ aller Automorphismen σ der Ordnung 2 einer endlichen elementaren abelschen Gruppe G vom Rang n und für die Primzahl p dann natürlich auch die Anzahl aller Lösungen von (3).
Die bei den folgenden Ausführungen angewendeten Methoden sind durchweg von elementarem Charakter und erfordern eine gesonderte Behandlung der Fälle $p \neq 2$ und $p = 2$.

§ 1. Charakterisierung der Automorphismen der Ordnung 2 von G im Fall $p \neq 2$

Es sei jetzt G eine endliche elementare abelsche Gruppe vom Rang $n \geqq 1$ für die Primzahl $p \neq 2$. Ferner sei σ ein Automorphismus der Ordnung 2 von G. Durch σ lassen sich jetzt zwei Mengen von Elementen aus G definieren.

Definition 1. U_σ sei die Menge aller $a \in G$ mit $\sigma(a) = a$.

U_σ ist nicht leer, da sicher $0 \in U_\sigma$ ist.

Definition 2. U'_σ sei die Menge aller $b \in G$ mit $b + \sigma(b) = 0$.

Auch U'_σ ist nicht leer, da sicher $0 \in U'_\sigma$ ist.
Es gelten nun die folgenden beiden Sätze.

Satz 1. *Ist σ ein Automorphismus der Ordnung 2 von G, so sind U_σ und U'_σ Untergruppen von G.*

Beweis. Für U_σ gilt $0 \in U_\sigma$, weil $\sigma(0) = 0$ ist. Ist $a \neq 0$ und $a \in U_\sigma$, so ist auch $-a \in U_\sigma$, weil $\sigma(-a) = -\sigma(a) = -a$ ist. Ist $a \in U_\sigma$ und $b \in U_\sigma$, so ist $\sigma(a + b) = \sigma(a) + \sigma(b) = a + b$, also ist auch $a + b \in U_\sigma$. Für U'_σ gilt $0 \in U'_\sigma$, weil $0 + \sigma(0) = 0 + 0 = 0$ ist. Ist $a \neq 0$ und $a \in U'_\sigma$, so ist auch $-a \in U'_\sigma$ wegen $(-a) + \sigma(-a) = -\big(a + \sigma(a)\big) = 0$. Ist $a \in U'_\sigma$ und $b \in U'_\sigma$, so ist

$$(a + b) + \sigma(a + b) = \big(a + \sigma(a)\big) + \big(b + \sigma(b)\big) = 0 + 0 = 0,$$

also ist auch $a + b \in U'_\sigma$.

Satz 2. *Ist σ ein Automorphismus der Ordnung 2 von G, so ist G die direkte Summe der beiden Untergruppen U_σ und U'_σ von G, d. h., es ist $G = U_\sigma \dotplus U'_\sigma$.*

Beweis. Zunächst ist $U_\sigma \cap U'_\sigma = \{0\}$: Es sei $U_\sigma \cap U'_\sigma = D$ und $d \in D$. Wegen $d \in U_\sigma$ folgt $\sigma(d) = d$, und wegen $d \in U'_\sigma$ folgt $d + \sigma(d) = 0$. Also gilt $d + \sigma(d) = d + d = 2d = 0$. Da wegen $p \neq 2$ die Gruppe G und damit erst recht die Untergruppe U_σ von G kein Element der Ordnung 2 enthält, ist also $d = 0$. Weiter ist $G = U_\sigma + U'_\sigma$: Dazu genügt es zu zeigen, daß jedes Element $g \in G$ in der Form $g = u + u'$ mit $u \in U_\sigma$ und $u' \in U'_\sigma$ darstellbar ist. Das ist aber sicher der Fall, wenn in jeder Klasse $K \in G/U'_\sigma$ wenigstens ein Element $u \in U_\sigma$ liegt. Denn ist $g \in G$ beliebig, so kommt g in irgendeiner Klasse $K \in G/U'_\sigma$ vor. Da es dann aber in K auch ein Element $u \in U_\sigma$ gibt, existiert dazu sicher ein $u' \in U'_\sigma$, so daß $g = u + u'$ ist. Es sei also K eine beliebige Klasse aus G/U'_σ und $c \in K$. Sicher gilt allgemein $\sigma(c) = c + g$ mit passendem $g \in G$. Dann ist aber $c = \sigma\big(\sigma(c)\big) = \sigma(c) + \sigma(g) = c + g + \sigma(g)$, also $g + \sigma(g) = 0$, d. h., es ist $g \in U'_\sigma$. Also liegen c und $\sigma(c)$ für jedes $c \in G$ in derselben Klasse $K \in G/U'_\sigma$. Wegen $p \neq 2$ ist die Ordnung $o(G)$ von G ungerade. [Mit $o(\ldots)$ werde immer die Ordnung von $(\ldots)$ bezeichnet.] Die Anzahl der Elemente von U'_σ und damit die Anzahl der Elemente einer jeden Klasse $K \in G/U'_\sigma$ ist daher gleichfalls ungerade. Da nun $\sigma\big(\sigma(c)\big) = c$ ist, muß es also mindestens ein Element u aus K geben, für das $\sigma(u) = u$ gilt, das also aus U_σ stammt. Mithin ist $G = U_\sigma + U'_\sigma$. Aus $G = U_\sigma + U'_\sigma$ folgt zusammen mit $U_\sigma \cap U'_\sigma = \{0\}$, daß G die direkte Summe $G = U_\sigma \dotplus U'_\sigma$ der Untergruppen U_σ und U'_σ ist.

Bemerkung 1. Der identische Automorphismus $\sigma = \varepsilon$ von G kann auch als Automorphismus der Ordnung 2 von G aufgefaßt werden. Die zugehörige Matrix $\mathfrak{A}_n$ ist in diesem Fall die Einheitsmatrix $\mathfrak{E}_n$. ε entspricht dann offenbar die direkte Summe $G = G \dotplus \{0\}$.

Durch $\tau(a_i) = -a_i = (p-1)\,a_i$ ($a_1, \ldots, a_n$ Basis von G) wird ein Automorphismus der Ordnung 2 von G definiert. Die zugehörige Matrix $\mathfrak{A}_n$ besitzt nämlich die Form

$$\mathfrak{A}_n = \begin{pmatrix} p-1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & p-1 \end{pmatrix}, \tag{4}$$

und wegen $(p-1)^2 = p^2 - 2p + 1 \equiv 1 \bmod p$ gilt sicherlich $\mathfrak{A}_n^2 \equiv \mathfrak{E}_n \bmod p$. τ entspricht dann offenbar die direkte Summe $G = \{0\} \dotplus G$.

Umgekehrt gilt aber auch der folgende Satz.

Satz 3. *Ist $G = U \dotplus U'$ direkte Summe der Untergruppen U und U' von G, so läßt sich ein Automorphismus σ der Ordnung 2 von G auf folgende Weise definieren: Ist $\{0\} \subset U \subset G$, $a_1, \ldots, a_k$ eine beliebige Basis von U, $b_1, \ldots, b_m$ eine beliebige Basis von U', so sei $\sigma(a_i) = a_i$, $i = 1, \ldots, k$, und $\sigma(b_j) = -b_j$, $j = 1, \ldots, m$. Ist $U = \{0\}$, also $U' = G$, so sei $\sigma(b_j) = -b_j$, $j = 1, \ldots, n$, für eine beliebige Basis von G. Ist $U = G$, also $U' = \{0\}$, so sei $\sigma(a_i) = a_i$, $i = 1, \ldots, n$, für eine beliebige Basis von G.*

Beweis. Offenbar bilden im Fall $\{0\} \subset U \subset G$ die Elemente $a_1, \ldots, a_k$ und $b_1, \ldots, b_m$ zusammen eine Basis von G. σ ist dann sicher ein Automorphismus der Ordnung 2 von G, denn σ entspricht die Matrix

$$\mathfrak{A}_n = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & p-1 & \\ & & & & \ddots \\ 0 & & & & p-1 \end{pmatrix}, \tag{5}$$

für die wegen $1 \cdot 1 \equiv 1 \bmod p$ und $(p-1)^2 \equiv 1 \bmod p$ die Eigenschaft (2) gilt. Im Fall $U' = G$ ist σ der Automorphismus τ aus Bemerkung 1 und im Fall $U = G$ der identische Automorphismus ε.

Bemerkung 2. Da bei jeder Wahl der a_i bzw. b_j jedes Element von U durch σ in sich bzw. jedes Element von U' durch σ in das inverse Element übergeführt wird, ist die Definition von σ nur von U und U', aber nicht von der Wahl der Basen in U bzw. U' abhängig. Selbstverständlich ist dann auch $U = U_\sigma$ und $U' = U'_\sigma$.

Auf Grund der Sätze 2 und 3 und der im Anschluß an diese Sätze gemachten Bemerkungen 1 und 2 gilt also der folgende Satz.

Satz 4. *Der Gesamtheit der Automorphismen σ der Ordnung 2 von G entspricht im Fall $p \neq 2$ in eineindeutiger Weise die Gesamtheit der Darstellungen von G als direkte Summe $G = U \dotplus U'$ zweier Untergruppen U und U' von G unter Berücksichtigung der Reihenfolge der Summanden, wobei jeweils U die Gesamtheit der Elemente g von G mit $\sigma(g) = g$ und U' die Gesamtheit der Elemente g' von G mit $\sigma(g') = -g'$ ist.*

§ 2. Charakterisierung der Automorphismen der Ordnung 2 von G im Fall $p = 2$

Es sei jetzt G eine endliche elementare abelsche Gruppe vom Rang $n \geqq 1$ für die Primzahl $p = 2$. Ferner sei σ ein Automorphismus der Ordnung 2 von G. Wie in Definition 2 werde auch jetzt definiert:

Definition 3. U'_σ sei die Menge aller $b \in G$ mit $b + \sigma(b) = 0$.

U'_σ ist nicht leer, da sicher $0 \in U'_\sigma$ ist. Es ließe sich natürlich auch eine Untergruppe U_σ wie in Definition 1 definieren, allerdings wäre dann $U_\sigma = U'_\sigma$, da alle Elemente g von G jetzt die Ordnung $o(g) = 2$ besitzen und aus $g + \sigma(g) = 0$ sofort $\sigma(g) = -g = g$ und umgekehrt folgen würde.

Für U'_σ gilt zunächst wie im Fall $p \neq 2$ der folgende Satz.

Satz 5. *Ist σ ein Automorphismus der Ordnung 2 von G, so ist U'_σ eine Untergruppe von G.*

Beweis. Wie bei Satz 1.

Im Gegensatz zum Fall $p \neq 2$ gilt jetzt aber

Satz 6. *Es ist stets* $\{0\} \subset U'_\sigma$.

Beweis. Angenommen, es sei $U'_\sigma = \{0\}$. Dann wäre $a + \sigma(a) \neq 0$, d. h. $\sigma(a) \neq a$ für jedes $a \neq 0$ aus G. Zu jedem $a \neq 0$ aus G würde also genau ein Element $\sigma(a) \neq a$ aus G gehören, und wegen $\sigma\big(\sigma(a)\big) = a$ und $\sigma(0) = 0$ müßte die Ordnung $o(G)$ von G ungerade sein. Das ist aber ein Widerspruch, denn wegen $p = 2$ ist 2 ein Teiler von $o(G)$.

Es werde nun die Faktorgruppe G/U'_σ betrachtet. Es sei K eine beliebige Klasse von G/U'_σ und g ein beliebiges Element von K. Dann ist $g + \sigma(g) \in U'_\sigma$, denn es ist

$$\begin{aligned}&\big(g + \sigma(g)\big) + \sigma\big(g + \sigma(g)\big)\\ &= g + \sigma(g) + \sigma(g) + \sigma\big(\sigma(g)\big)\\ &= g + 2\sigma(g) + g = 2g + 2\sigma(g) = 0 + 0 = 0.\end{aligned}$$

Es sei jetzt $g' \neq g$ aus K. Dann ist $g' = g + u'$ mit $u' \in U'_\sigma$ und

$$\begin{aligned}g' + \sigma(g') &= g + u' + \sigma(g + u') = g + u' + \sigma(g) + \sigma(u')\\ &= g + u' + \sigma(g) + \sigma(u') = g + \sigma(g),\end{aligned}$$

weil $u' + \sigma(u') = 0$ ist wegen $u' \in U'_\sigma$.
Wegen $g + \sigma(g) \in U'_\sigma$ und $g + \sigma(g) = g' + \sigma(g')$ kann also jeder Klasse $K \in G/U'_\sigma$ eindeutig ein Element $a = g + \sigma(g) \in U'_\sigma$ zugeordnet werden, wobei g beliebig aus K gewählt sein kann. Für diese Zuordnung gilt nun

Satz 7. *Die Abbildung $\varphi(K) = g + \sigma(g)$ [$K \in G/U'_\sigma$, g beliebig aus K] ist ein Homomorphismus von G/U'_σ in U'_σ.*

Beweis. Wie bereits oben gezeigt, ist $\varphi(K) \in U'_\sigma$ unabhängig von der Wahl von g. Es seien nun $K_1, K_2 \in G/U'_\sigma$. Dann ist $\varphi(K_1 + K_2) = (k_1 + k_2) + \sigma(k_1 + k_2)$ für beliebige $k_1 \in K_1$, $k_2 \in K_2$, also ist $\varphi(K_1 + K_2) = \big(k_1 + \sigma(k_1)\big) + \big(k_2 + \sigma(k_2)\big) = \varphi(K_1) + \varphi(K_2)$.
Da aus $\varphi(K) = 0$ aber $\varphi(K) = \big(g + \sigma(g)\big) = 0$ ($g \in K$), d. h. $g \in U'_\sigma$, also $K = U'_\sigma$ folgt, ist vermöge φ natürlich G/U'_σ einer Untergruppe U^*_σ von U'_σ isomorph, d. h., es gilt $G/U'_\sigma \cong U^*_\sigma$ mit $U^*_\sigma \subseteq U'_\sigma$. Aus $G/U'_\sigma \cong U^*_\sigma$ folgt weiter, daß $o(U'_\sigma) \cdot o(U^*_\sigma) = o(G)$ für die Ordnungen der betreffenden Gruppen gelten muß.

Zusammenfassend gilt also der folgende Satz.

Satz 8. *Ist σ ein Automorphismus der Ordnung 2 von G, so werden durch σ festgelegt:*
1. *Eine Untergruppe U'_σ von G mit* $\{0\} \subset U'_\sigma$ [U'_σ *Menge aller $g \in G$ mit $g + \sigma(g) = 0$*].

2. *Eine Untergruppe U_σ^* von G mit $U_\sigma^* \subseteqq U'_\sigma$ und $o(U'_\sigma) \cdot o(U_\sigma^*) = o(G)$ [U_σ^* Menge aller verschiedenen Elemente der Form $g + \sigma(g)$ aus G].*
3. *Ein Isomorphismus φ von G/U'_σ auf U_σ^* vermöge $\varphi(K) = g + \sigma(g) \in U_\sigma^*$ [$K \in G/U'_\sigma$, g beliebig aus K].*

Bemerkung 3. Ist φ der durch σ bestimmte Isomorphismus von G/U'_σ auf U_σ^*, so gilt natürlich auch $\sigma(g) = g + \varphi\big(K(g)\big)$, g beliebig aus G, und $K(g)$ ist die Klasse von G/U'_σ, in der das Element $g \in G$ liegt.

Nun besteht aber auch umgekehrt der folgende Satz.

Satz 9. *Es seien $U' \neq \{0\}$ und U^* zwei Untergruppen von G mit $U^* \subseteqq U'$ und $o(U^*) \cdot o(U') = o(G)$. Ferner sei φ ein Isomorphismus von G/U' auf U^*. Dann wird durch $\sigma(g) = g + \varphi\big(K(g)\big)$ [$g \in G$, $K(g)$ Klasse von G/U', in der g liegt] ein Automorphismus der Ordnung 2 von G definiert.*

Beweis. Da der Typus von G/U' wegen $o(U^*) \cdot o(U') = o(G)$ offenbar gleich dem Typus von U^* ist, sind G/U' und U^* isomorph. Es sei nun φ ein Isomorphismus von G/U' auf U^*. Dann wird durch $\sigma(g) = g + \varphi\big(K(g)\big)$ ein Homomorphismus von G in sich definiert, denn es ist

$$\begin{aligned}\sigma(g_1 + g_2) &= (g_1 + g_2) + \varphi\big(K(g_1 + g_2)\big)\\ &= \big[g_1 + \varphi\big(K(g_1)\big)\big] + \big[g_2 + \varphi\big(K(g_2)\big)\big] = \sigma(g_1) + \sigma(g_2)\end{aligned}$$

(g_1, g_2 beliebig aus G). Es sei nun $\sigma(g) = g + \varphi\big(K(g)\big) = 0$, also $\varphi\big(K(g)\big) = g \in U^* \subseteqq U'$. Die Klasse, in der g liegt, ist also gleich U', d. h., es ist $K(g) = U'$. Da aber U' das Nullelement von G/U' ist, muß $\varphi\big(K(g)\big) = 0$ gelten, weil φ ein Isomorphismus ist. Folglich ist $\sigma(g) = g = 0$. Der Kern von σ ist somit $\{0\}$, d. h., σ ist ein Isomorphismus von G auf sich, d. h. ein Automorphismus von G. Weiter ist

$$\begin{aligned}\sigma\big(\sigma(g)\big) &= \sigma\big[g + \varphi\big(K(g)\big)\big] = \sigma(g) + \sigma\big[\varphi\big(K(g)\big)\big]\\ &= \sigma(g) + \varphi\big(K(g)\big) + \varphi\big[K\big(\varphi(K(g))\big)\big].\end{aligned}$$

Da $\varphi\big(K(g)\big) \in U^* \subseteqq U'$ gilt, ist $K\big(\varphi(K(g))\big) = U'$ und daher $\varphi\big[K\big(\varphi(K(g))\big)\big] = \varphi(U') = 0$. Also ist

$$\sigma\big(\sigma(g)\big) = \sigma(g) + \varphi\big(K(g)\big) = g + \varphi\big(K(g)\big) + \varphi\big(K(g)\big) = g,$$

da $o\big(\varphi(K(g))\big) = 2$ wegen $p = 2$ ist. Mithin ist σ ein Automorphismus der Ordnung 2.

Auf Grund der Sätze 6 und 7 und der im Anschluß an Satz 6 gemachten Bemerkung 3 gilt also der folgende Satz.

Satz 10. *Der Gesamtheit der Automorphismen σ der Ordnung 2 von G entspricht im Fall $p = 2$ in eineindeutiger Weise die Gesamtheit der Tripel (U', U^*, φ), wobei U', U^* ein Untergruppenpaar von G mit $\{0\} \subset U'$, $U^* \subseteqq U'$, $o(U^*) \cdot o(U') = o(G)$ und φ ein Isomorphismus von G/U' auf U^* ist. U' ist dabei die Gesamtheit aller $g \in G$ mit $g + \sigma(g) = 0$, U^* die Gesamtheit aller verschiedenen Elemente der Form $g + \sigma(g)$ aus G und φ ein Isomorphismus von G/U' auf U^*, so daß für $g \in G$ und $K(g) \in G/U'$ [$K(g)$ Klasse von G/U', in der das Element g liegt] gerade $g + \sigma(g) = \varphi\big(K(g)\big)$ gilt.*

§ 3. Bestimmung aller Untergruppen U von G für eine beliebige Primzahl p

Um die Automorphismen der Ordnung 2 einer endlichen elementaren abelschen Gruppe G vom Rang $n \geqq 1$ für die Primzahl p zu bestimmen, ist es nach den Sätzen 4 und 10 sowohl für den Fall $p \neq 2$ als auch für den Fall $p = 2$ erforderlich, sich erst

einmal einen Überblick über alle Untergruppen von G zu verschaffen. p sei jetzt also eine beliebige Primzahl. Zunächst kann festgestellt werden, daß es im Fall $n = 1$ nur die trivialen Untergruppen $\{0\}$ und G von G gibt, während im Fall $n > 1$ nichttriviale Untergruppen von G existieren, bei denen als Ordnungen wegen $o(G) = p^n$ nur die Zahlen $p^1, p^2, \ldots, p^{n-1}$ auftreten können und daß ferner wegen $o(b) = p$ für alle $b \neq 0$ aus G als Typus von U nur die Möglichkeiten (p), (p, p), $\ldots$, $(p, p, \ldots, p,$ $(n-1)$-mal) in Betracht kommen. Im folgenden werde daher $n > 1$ angenommen. Bilden die Elemente $a_1, \ldots, a_n$ mit $o(a_i) = p$, $i = 1, \ldots, n$, eine Basis von G, so läßt sich jedes Element b von G eindeutig in der Form $b = k_1 a_1 + \cdots + k_n a_n$ schreiben, wobei die k_i ganze Zahlen mit $0 \leqq k_i \leqq p - 1$ sind. Hat bezüglich der festen Basis $a_1, \ldots, a_n$ das Element b die Darstellung $b = k_1 a_1 + \cdots + k_n a_n$, so soll in Zukunft dafür kürzer

$$b = (k_1, \ldots, k_n), \quad 0 \leqq k_i \leqq p - 1, \quad i = 1, \ldots, n, \tag{6}$$

geschrieben werden.

Für das weitere sind die beiden folgenden Definitionen nützlich.

Definition 4. Ein Element ungleich dem Nullelement von G heiße *von der Form t (bezüglich der Basis $a_1, \ldots, a_n$)* und werde mit $b_t^{(t)}$, $t = 1, \ldots, n$, bezeichnet, wenn es die folgende Gestalt besitzt:

$$b_t^{(t)} = (0, \ldots, 0, 1, k_{t+1}^{(t)}, \ldots, k_n^{(t)}). \tag{7}$$

Die 1 steht dabei an t-ter Stelle, und es gilt $0 \leqq k_j^{(t)} \leqq p - 1$ für $j = t + 1, \ldots, n$. Ist $t > 1$, so stehen links von der Eins stets lauter Nullen.

Definition 5. T sei eine beliebige geordnete nichttriviale Teilmenge von $\{1, 2, \ldots, n\}$, also

$$T = \{t_1, t_2, \ldots, t_m\}, \quad m = 1, 2, \ldots, n - 1, \quad 1 \leqq t_1 < t_2 < \cdots < t_m \leqq n. \tag{8}$$

Die Elemente $B_1, B_2, \ldots, B_m$ von G bilden dann eine T-Menge $\mathfrak{T}$ (bezüglich der Basis $a_1, \ldots, a_n$), wenn sie von der Form t_1 bzw. t_2 bzw. $\ldots$ bzw. t_m sind, also das Aussehen

$$B_i = b_{t_i}^{(i)} = (0, \ldots, 0, 1, k_{t_i+1}^{(i)}, \ldots, k_n^{(i)}), \quad i = 1, \ldots, m, \tag{9}$$

besitzen, und wenn außerdem $k_{t_l}^{(i)} = 0$ für $t_l > t_i$ gilt, falls $t_l \in T$ ist.

Beispiel. G sei vom Typus (3, 3, 3, 3, 3), also $p = 3$, $n = 5$. Ferner sei $T = \{1, 3, 5\}$, also $m = 3$, $t_1 = 1$, $t_2 = 3$, $t_3 = 5$. Dann ist

$$B_1 = b_{t_1}^{(1)} = b_1^{(1)} = (1, k_2^{(1)}, k_3^{(1)}, k_4^{(1)}, k_5^{(1)}) = (1, \alpha, 0, \beta, 0),$$

$$B_2 = b_{t_2}^{(2)} = b_3^{(2)} = (0, 0, 1, k_4^{(2)}, k_5^{(2)}) = (0, 0, 1, \gamma, 0),$$

$$B_3 = b_{t_3}^{(3)} = b_5^{(3)} = (0, 0, 0, 0, 1) = (0, 0, 0, 0, 1), \quad 0 \leqq \alpha, \beta, \gamma \leqq 2,$$

also z. B.

$$B_1 = (1, 2, 0, 2, 0),$$

$$B_2 = (0, 0, 1, 1, 0),$$

$$B_3 = (0, 0, 0, 0, 1).$$

Für T-Mengen gelten nun die folgenden Sätze.

Satz 11. *Die Elemente einer T-Menge $\mathfrak{T}$ sind linear unabhängig.*

Beweis. Es sei $T = \{t_1, t_2, \ldots, t_m\}$ mit $1 \leqq m \leqq n-1$, $1 \leqq t_1 < t_2 < \cdots < t_m \leqq n$. Eine entsprechende T-Menge $\mathfrak{T}$ werde von den Elementen

$$B_i = b_{t_i}^{(i)} = (0, \ldots, 0, 1, k_{t_i+1}^{(i)}, \ldots, k_n^{(i)}), \tag{10}$$

die 1 steht an der Stelle t_i, $i = 1, \ldots, m$, gebildet. Angenommen, es sei $\alpha_1 B_1 + \alpha_2 B_2 + \cdots + \alpha_m B_m = 0$ (α_i ganz, $0 \leqq \alpha_i \leqq p-1$). Dann ist aber auf Grund der Festlegung über die $k_{t_j}^{(i)}$ gemäß Definition 5

$$\begin{aligned} \alpha_1 B_1 + \alpha_2 B_2 + \cdots + \alpha_m B_m &= (0, \ldots, 0, \alpha_1, \ldots, \alpha_2, \ldots, \alpha_m, \ldots) \\ &= (0, \ldots, 0, 0, \ldots, 0, \ldots, 0, \ldots), \end{aligned} \tag{11}$$

also $\alpha_1 = \alpha_2 = \cdots = \alpha_m = 0$, d. h., die B_i sind linear unabhängig.

Bemerkung 4. Da die Elemente einer T-Menge $\mathfrak{T}$ nach obigem Satz 11 linear unabhängig sind, können sie als Basis der von ihnen erzeugten Untergruppe U von G aufgefaßt werden.

Satz 12. *Zwei verschiedene T-Mengen erzeugen auch zwei verschiedene Untergruppen von G.*

Beweis. Es seien $\mathfrak{A} = \{B_1, B_2, \ldots, B_m\}$ und $\mathfrak{B} = \{B_1^*, B_2^*, \ldots, B_s^*\}$ zwei verschiedene T-Mengen. $\mathfrak{A}$ erzeuge die Untergruppe U von G und $\mathfrak{B}$ die Untergruppe V von G. Dabei bilden laut Bemerkung 4 die B_i eine Basis von U und die B_j^* eine Basis von V. Angenommen, es sei $U = V$. Dann muß aber $s = m$ sein, da Basen unterschiedlicher Länge sicherlich verschiedene Untergruppen erzeugen. Eine Linearkombination aus $B_1^*, B_2^*, \ldots, B_m^*$ hat offenbar die Gestalt

$$\beta_1^* B_1^* + \beta_2^* B_2^* + \cdots + \beta_m^* B_m^* = (0, \ldots, 0, \beta_1^*, \ldots, \beta_2^*, \ldots, \beta_m^*, \ldots), \tag{12}$$

wobei die β_i^* an den Stellen t_i^*, $i = 1, \ldots, m$, stehen und links von β_1^* nur Nullen auftreten. B_1 ist von der Form

$$B_1 = (0, \ldots, 0, 1, \ldots, 0, \ldots, 0, \ldots), \tag{13}$$

wobei die 1 an der Stelle t_1 steht, an den Stellen t_i, $i = 2, \ldots, m$, jeweils eine Null auftritt und links von der 1 nur Nullen vorkommen. Da $U = V$ sein soll, muß sich B_1 auch in der Form (12) darstellen lassen. Auf Grund der rechten Seiten von (12) und (13) folgt, daß nicht $t_1 < t_1^*$ gelten kann. Es kann aber auch nicht $t_1^* < t_1$ sein, was sich aus einer entsprechenden Überlegung für $B_1, \ldots, B_m$ und B_1^* folgern ließe. Es muß also $t_1 = t_1^*$ gelten. Nun ist

$$B_2 = (0, \ldots, 0, 1, \ldots, 0, \ldots, 0, \ldots), \tag{14}$$

wobei die 1 an der Stelle t_2 steht, an den Stellen t_i, $i = 3, \ldots, m$, jeweils eine Null auftritt und links von der 1 nur Nullen vorkommen. Wird B_2 in der Form (12) dargestellt, so muß, da in (14) an der Stelle t_1 eine Null steht, wegen $t_1^* = t_1 < t_2$ in (12) natürlich $\beta_1^* = 0$ sein. Damit gilt dann

$$(0, \ldots, 0, 1, \ldots, 0, \ldots, 0, \ldots) = (0, \ldots, 0, \beta_2^*, \ldots, \beta_3^*, \ldots, \beta_m^*, \ldots), \tag{15}$$

wobei in (15) die 1 an der Stelle t_2 und β_2^* an der Stelle t_2^* steht. Die Nullen rechts von der 1 stehen an den Stellen t_i, $i = 3, \ldots, m$, und die β_j^* rechts von β_2^* an den Stellen t_j^*, $j = 3, \ldots, m$. Links von der 1 bzw. links von β_2^* treten nur Nullen auf. Wie vorher ergibt sich dann, daß $t_2 = t_2^*$ gelten muß. Wird diese Schlußweise fortgesetzt, so erhält man nacheinander $t_3 = t_3^*, \ldots, t_m = t_m^*$. Wird jetzt B_1 in der Form (12) dargestellt, so folgt aus (13) natürlich sofort $\beta_1^* = 1$ und $\beta_2^* = \cdots = \beta_m^* = 0$, also $B_1 = B_1^*$.

Wird B_2 in der Form (12) dargestellt, so ergibt sich entsprechend aus (15) ebenfalls sofort $\beta_1^* = 0$, $\beta_2^* = 1$, $\beta_3^* = \cdots = \beta_m^* = 0$, also $B_2 = B_2^*$. So fortfahrend erhält man weiter nacheinander $B_3 = B_3^*, \ldots, B_m = B_m^*$. Damit würden $\mathfrak{A}$ und $\mathfrak{B}$ übereinstimmen, was im Widerspruch zur Voraussetzung steht. Zwei verschiedene T-Mengen erzeugen also auch zwei verschiedene Untergruppen von G.

Satz 13. *Jede echte Untergruppe U von G läßt sich durch eine T-Menge erzeugen.*

Beweis. Für den Beweis von Satz 13 werden die folgenden beiden Hilfssätze benötigt, die in allgemeinerer Form in einer früheren Arbeit ([2], Hilfssatz 1, S. 102, Hilfssatz 2, S. 103) bewiesen wurden. Hier sollen diese Hilfssätze nur in der erforderlichen speziellen Form aufgeführt werden.

Hilfssatz 1. *Ist $u_1, \ldots, u_m$ eine Basis von U, so auch $u_1, \ldots, \alpha u_i, \ldots, u_m$ für jedes i, $i = 1, \ldots, m$, und für jedes ganze α mit $0 < \alpha \leqq p - 1$.*

Hilfssatz 2. *Ist $u_1, \ldots, u_i, \ldots, u_j, \ldots, u_m$ eine Basis von U, dann auch $u_1, \ldots, u_i, \ldots, \alpha u_i + u_j, \ldots, u_m$ für jedes i, $i = 1, \ldots, m$, und jedes $j \neq i$, $j = 1, \ldots, m$, und für jedes ganze α mit $0 \leqq \alpha \leqq p - 1$.*

Es sei nun $a_1, \ldots, a_n$ eine Basis von G, $u_1, \ldots, u_m$ eine Basis von U. Dann ist $u_i = (\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{in})$, $i = 1, \ldots, m$, oder als Matrix geschrieben:

$$\mathfrak{A}_{m,n} = \begin{pmatrix} \alpha_{11} \alpha_{12} \cdots \alpha_{1n} \\ \alpha_{21} \alpha_{22} \cdots \alpha_{2n} \\ \vdots \quad \vdots \quad \quad \vdots \\ \alpha_{m1} \alpha_{m2} \cdots \alpha_{mn} \end{pmatrix}, \tag{16}$$

wobei die α_{ik} natürlich immer als ganze nichtnegative Zahlen mod p zu verstehen sind. Da die u_i eine Basis von U darstellen, können in $\mathfrak{A}_{m,n}$ keine Nullzeilen auftreten. Die j-te Spalte sei nun die erste Spalte von $\mathfrak{A}_{m,n}$, in der ein von Null verschiedenes Element steht, und es sei z. B. $\alpha_{ij} \neq 0$. Dann vertausche man die i-te Zeile mit der ersten. Weiter gibt es sicher ein α mit $0 < \alpha \leqq p - 1$, so daß $\alpha\alpha_{ij} \equiv 1 \bmod p$ wird. Die neue erste Zeile wird dann mit α multipliziert. Nach Hilfssatz 1 stellen die Zeilen der auf diese Weise erhaltenen Matrix wieder eine Basis von U dar. Addiert man nun passende Multipla der ersten Zeile zu den übrigen — zur l-ten Zeile z. B. addiere man die mit $p - \alpha_{lj}$ multiplizierte erste Zeile — so läßt sich erreichen, daß, die erste Stelle ausgenommen, sonst an jeder anderen Stelle der j-ten Spalte eine Null steht. Nach Hilfssatz 2 stellen auch jetzt die Zeilen der so entstandenen Matrix $\mathfrak{A}'_{m,n}$ eine Basis von U dar. $\mathfrak{A}'_{m,n}$ hat das folgende Aussehen:

$$\mathfrak{A}'_{m,n} = \begin{pmatrix} 0 \ldots 0 \; 1 \; \alpha'_{1,j+1} \cdots \alpha'_{1n} \\ 0 \ldots 0 \; 0 \; \alpha'_{2,j+1} \cdots \alpha'_{2n} \\ \vdots \quad \vdots \; \vdots \; \vdots \quad \quad \vdots \\ 0 \ldots 0 \; 0 \; \alpha'_{m,j+1} \cdots \alpha'_{mn} \end{pmatrix}. \tag{17}$$

Nun werden dieselben Schritte, die von $\mathfrak{A}_{m,n}$ zu $\mathfrak{A}'_{m,n}$ führten, bei der Matrix

$$\mathfrak{B}'_{m-1,n-j} = \begin{pmatrix} \alpha_{2,j+1} \cdots \alpha'_{2n} \\ \vdots \quad \quad \vdots \\ \alpha'_{m,j+1} \cdots \alpha'_{mn} \end{pmatrix} \tag{18}$$

ausgeführt. Als Resultat erhält man dann eine Matrix der Form

$$\mathfrak{B}^{*}_{m-1,n-j} = \begin{pmatrix} 0 \dots 0 & 1 & \alpha''_{2,k+1} \dots \alpha''_{2n} \\ 0 \dots 0 & 0 & \alpha''_{3,k+1} \dots \alpha''_{3n} \\ \vdots & \vdots & \vdots \\ 0 \dots 0 & 0 & \alpha''_{m,k+1} \dots \alpha''_{mn} \end{pmatrix}. \tag{19}$$

Setzt man jetzt $\mathfrak{B}^{*}_{m-1,n-j}$ statt $\mathfrak{B}'_{m-1,n-j}$ in $\mathfrak{A}'_{m,n}$ ein und addiert noch ein passendes Multiplum der ersten Zeile von $\mathfrak{B}^{*}_{m-1,n-j}$ zu der ersten Zeile von $\mathfrak{A}'_{m,n}$, so läßt sich $\mathfrak{A}'_{m,n}$ auf die folgende Gestalt bringen:

$$\mathfrak{A}''_{m,n} = \begin{pmatrix} 0 \dots 0 & 1 & \alpha'_{1,j+1} \dots \alpha'_{1,k-1} & 0 & \alpha''_{1,k+1} \dots \alpha''_{1n} \\ 0 \dots 0 & 0 & 0 \dots 0 & 1 & \alpha''_{2,k+1} \dots \alpha''_{2n} \\ 0 \dots 0 & 0 & 0 \dots 0 & 0 & \alpha''_{3,k+1} \dots \alpha''_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 \dots 0 & 0 & 0 \dots 0 & 0 & \alpha''_{m,k+1} \dots \alpha''_{mn} \end{pmatrix}. \tag{20}$$

Die Zeilen von $\mathfrak{A}''_{m,n}$ stellen auf Grund der Hilfssätze 1 und 2 wieder eine Basis von U dar. Nun betrachtet man die Matrix

$$\mathfrak{B}''_{m-2,n-k} = \begin{pmatrix} \alpha''_{3,k+1} \dots \alpha''_{3n} \\ \vdots \\ \alpha''_{m,k+1} \dots \alpha''_{mn} \end{pmatrix} \tag{21}$$

und verfährt in derselben Weise wie oben mit der Matrix $\mathfrak{A}_{m,n}$. Die der Matrix $\mathfrak{B}^{*}_{m-1,n-j}$ entsprechende Matrix $\mathfrak{B}^{**}_{m-2,n-k}$ wird dann in $\mathfrak{A}''_{m,n}$ eingesetzt, und durch Addition passender Multipla der ersten Zeile von $\mathfrak{B}^{**}_{m-2,n-k}$ wird dafür gesorgt, daß $\mathfrak{A}''_{m,n}$ schließlich die Form

$$\mathfrak{A}'''_{m,n} = \begin{pmatrix} 0 \dots 0 & 1 & \alpha'_{1,j+1} \dots \alpha'_{1,k-1} & 0 & \alpha''_{1,k+1} \dots \alpha''_{1,l-1} & 0 & \alpha'''_{1,l+1} \dots \alpha'''_{1n} \\ 0 \dots 0 & 0 & 0 \dots 0 & 1 & \alpha''_{2,k+1} \dots \alpha''_{2,l-1} & 0 & \alpha'''_{2,l+1} \dots \alpha'''_{2n} \\ 0 \dots 0 & 0 & 0 \dots 0 & 0 & 0 \dots 0 & 1 & \alpha'''_{3,l+1} \dots \alpha'''_{3n} \\ 0 \dots 0 & 0 & 0 \dots 0 & 0 & 0 \dots 0 & 0 & \alpha'''_{4,l+1} \dots \alpha'''_{4n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 \dots 0 & 0 & 0 \dots 0 & 0 & 0 \dots 0 & 0 & \alpha'''_{m,l+1} \dots \alpha'''_{mn} \end{pmatrix} \tag{22}$$

annimmt, wobei die Zeilen von $\mathfrak{A}'''_{m,n}$ wieder eine Basis von U bilden. Nach endlich vielen Wiederholungen dieses Verfahrens erhält man so eine Matrix, deren Zeilen nach wie vor eine Basis von U darstellen, die Basiselemente jetzt aber offenbar eine T-Menge bilden. Damit ist Satz 13 bewiesen.

Auf Grund der Sätze 12 und 13 gilt also zusammenfassend der folgende Satz.

Satz 14. *Im Fall $n > 1$ entspricht der Gesamtheit der echten Untergruppen U von G nach Wahl einer festen Basis in G in eineindeutiger Weise die Gesamtheit aller T-Mengen aus Elementen von G. Dabei ist jede T-Menge Basis einer Untergruppe, und jede Untergruppe besitzt eine Basis, die eine T-Menge darstellt. Im Fall $n = 1$ existieren keine echten Untergruppen, sondern nur die trivialen Untergruppen $U = \{0\}$ und $U = G$ von G.*

Bemerkung 5. Im Beweis von Satz 13 wurde gezeigt, wie man von einer Basis von U zu einer T-Menge von U gelangen kann. Sicherlich läßt sich dasselbe Verfahren auch anwenden, wenn U nicht durch eine Basis, sondern durch ein Erzeugendensystem gegeben ist.

Beispiel. G sei vom Typus (5, 5, 5, 5, 5), also ist $p = 5$ und $n = 5$. Eine Untergruppe U von G werde von $u_1 = (2, 1, 3, 0, 2)$, $u_2 = (2, 0, 1, 1, 4)$, $u_3 = (4, 1, 4, 1, 1)$, $u_4 = (0, 0, 0, 1, 1)$ erzeugt. Offenbar bilden die u_i keine Basis von U, denn es ist, wie man leicht nachrechnet, z. B. $2u_1 + 2u_2 + 3u_3 + 0u_4 = 0$. Die Matrix

$$\mathfrak{A}_{4,5} = \begin{pmatrix} 2 & 1 & 3 & 0 & 2 \\ 2 & 0 & 1 & 1 & 4 \\ 4 & 1 & 4 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

mit den u_i als Zeilen kann dann wie folgt umgeformt werden (alle Rechnungen sind natürlich immer mod 5 durchzuführen):
Multiplikation der ersten Zeile mit 3 ergibt die Matrix

$$\begin{pmatrix} 1 & 3 & 4 & 0 & 1 \\ 2 & 0 & 1 & 1 & 4 \\ 4 & 1 & 4 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Addition der mit 3 multiplizierten ersten bzw. der mit 1 multiplizierten ersten Zeile zur zweiten bzw. zur dritten Zeile ergibt die Matrix

$$\begin{pmatrix} 1 & 3 & 4 & 0 & 1 \\ 0 & 4 & 3 & 1 & 2 \\ 0 & 4 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Offenbar kann hier z. B. die dritte Zeile gestrichen werden, und man erhält die Matrix

$$\begin{pmatrix} 1 & 3 & 4 & 0 & 1 \\ 0 & 4 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Multiplikation der zweiten Zeile mit 4 ergibt die Matrix

$$\begin{pmatrix} 1 & 3 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 3 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Addition der mit 2 multiplizierten zweiten Zeile zur ersten Zeile ergibt die Matrix

$$\begin{pmatrix} 1 & 0 & 3 & 3 & 2 \\ 0 & 1 & 2 & 4 & 3 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Addition der mit 2 multiplizierten dritten bzw. der mit 1 multiplizierten dritten Zeile zur ersten bzw. zur zweiten Zeile ergibt die Matrix

$$\mathfrak{B}_{3,5} = \begin{pmatrix} 1 & 0 & 3 & 0 & 4 \\ 0 & 1 & 2 & 0 & 4 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Die Zeilen von $\mathfrak{B}_{3,5}$ ergeben die folgenden Elemente $v_1 = (1, 0, 3, 0, 4)$, $v_2 = (0, 1, 2, 0, 4)$, $v_3 = (0, 0, 0, 1, 1)$ von G, die offenbar eine Basis von U bilden und in der Tat eine T-Menge darstellen.

§ 4. Aufstellung aller Darstellungen von G als direkte Summe zweier Untergruppen von G

Nach Satz 4 ist es im Fall $p \neq 2$ möglich, alle Automorphismen der Ordnung 2 von G zu konstruieren, wenn man alle Darstellungen von G als direkte Summe zweier Untergruppen von G angeben kann. Dies letztere soll jetzt im einzelnen behandelt werden. Dabei ist aber eine Einschränkung auf den Fall $p \neq 2$ nicht erforderlich, so daß in diesem Paragraphen p eine beliebige Primzahl sein kann. Zunächst gilt der folgende Satz.

Satz 15. *Jede Untergruppe U von G ist ein direkter Summand von G.*

Beweis. Für $U = G$ gilt die Behauptung mit $G = U \dotplus \{0\}$ und für $U = \{0\}$ mit $G = U \dotplus G$. Es sei jetzt also $\{0\} \subset U \subset G$ (und damit $n > 1$) und $u' \in G$, aber $u' \notin U$. Ist dann $U' = \{u'\}$ die von u' erzeugte zyklische Untergruppe von G, so gilt $U \cap U' = \{0\}$. Wäre nämlich $\alpha u' \in U$ mit $\alpha \not\equiv 0 \bmod p$, so müßte wegen $o(u') = p$ auch $u' \in U$ sein im Widerspruch zu $u' \notin U$. Ist nun $U \dotplus U' = G$, so ist alles gezeigt. Andernfalls existiert ein $u'' \in G$ mit $u'' \notin U \dotplus U'$. Ist dann $U'' = \{u''\}$ die von u'' erzeugte zyklische Untergruppe von G, so gilt $(U \dotplus U') \cap U'' = \{0\}$. Wäre nämlich $\beta u'' \in U \dotplus U'$ mit $\beta \not\equiv 0 \bmod p$, so müßte wegen $o(u'') = p$ auch $u'' \in U \dotplus U'$ sein im Widerspruch zu $u'' \notin U \dotplus U'$. Ist nun $(U \dotplus U') \dotplus U'' = U \dotplus (U' \dotplus U'') = U \dotplus U_1 = G$, so ist alles gezeigt. Andernfalls existiert ein $u''' \in G$ mit $u''' \notin U \dotplus U_1$ usw. Da G endlich ist, existiert also schließlich eine Untergruppe U_k von G mit $U \dotplus U_k = G$, d. h., U ist ein direkter Summand von G.

Nach Satz 15 gibt es also zu jeder beliebigen Untergruppe U von G eine Untergruppe U' von G mit $U \dotplus U' = G$. Da die Fälle $U = G$ und $U = \{0\}$ auf Grund von Bemerkung 1 und Satz 4 vollständig erledigt sind, kann im folgenden $\{0\} \subset U \subset G$ und damit $n > 1$ angenommen werden. Dann ist allerdings im Gegensatz zu den erledigten Fällen die Untergruppe U' in $U \dotplus U' = G$ nicht mehr eindeutig bestimmt. Man erhält aber zu gegebenem U mit $\{0\} \subset U \subset G$ sämtliche möglichen U' mit $U \dotplus U' = G$ auf Grund der beiden folgenden Sätze.

Satz 16. *Es sei U eine Untergruppe von G mit $\{0\} \subset U \subset G$ und $K_1 = r_1 + U$, $K_2 = r_2 + U, \ldots, K_m = r_m + U$ eine beliebige Basis von G/U, wobei die r_i beliebig aus den K_i, $i = 1, \ldots, m$, gewählt sein mögen. Ist dann U' eine Untergruppe von G mit $U \dotplus U' = G$, so gibt es immer passende Elemente $u_1^*, u_2^*, \ldots, u_m^*$ aus U, so daß die Elemente $r_1 + u_1^*, r_2 + u_2^*, \ldots, r_m + u_m^*$ eine Basis von U' bilden.*

Beweis. Es sei $K_1 = r_1 + U$, $K_2 = r_2 + U, \ldots, K_m = r_m + U$ eine Basis von G/U, r_i beliebig aus K_i, $i = 1, \ldots, m$. Wegen $U \dotplus U' = G$ gilt bekanntlich $G/U \cong U'$, und jedes Element aus U' kommt genau in einer Klasse von G/U vor. Also haben beispielsweise G/U und U' auch denselben Rang, und ist $r_1', r_2', \ldots, r_m'$ eine Basis von U', so ist $r_1' + U, r_2' + U, \ldots, r_m' + U$ eine weitere Basis von G/U. Dann gilt aber

$$\left.\begin{aligned} K_1 &= \alpha_{11}K_1' + \alpha_{12}K_2' + \cdots + \alpha_{1m}K_m', \\ K_2 &= \alpha_{21}K_1' + \alpha_{22}K_2' + \cdots + \alpha_{2m}K_m', \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ K_m &= \alpha_{m1}K_1' + \alpha_{m2}K_2' + \cdots + \alpha_{mm}K_m' \end{aligned}\right\} \tag{23}$$

mit eindeutig bestimmten ganzen α_{ik}, die der Bedingung $0 \leqq \alpha_{ik} \leqq p-1$ genügen. Da die K_i und die K'_j Basen von G/U darstellen, ist die Matrix $\mathfrak{A}_m$ der α_{ik} sicher nichtsingulär, d. h., es gibt eine Matrix $\mathfrak{B}_m$, deren Elemente β_{jl} ganz sind und der Bedingung $0 \leqq \beta_{jl} \leqq p-1$ genügen, mit $\mathfrak{A}_m \mathfrak{B}_m \equiv \mathfrak{E}_m \bmod p$. Aus (23) ergibt sich nun

$$\left.\begin{aligned} r_1 + u_1^* &= \alpha_{11} r'_1 + \alpha_{12} r'_2 + \cdots + \alpha_{1m} r'_m, \\ r_2 + u_2^* &= \alpha_{21} r'_1 + \alpha_{22} r'_2 + \cdots + \alpha_{2m} r'_m, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ r_m + u_m^* &= \alpha_{m1} r'_1 + \alpha_{m2} r'_2 + \cdots + \alpha_{mm} r'_m \end{aligned}\right\} \tag{24}$$

mit gewissen passenden $u_i^* \in U$. Da die Matrix $\mathfrak{A}_m$ der α_{ik} nichtsingulär ist, bilden dann die $r_i + u_i^*$, $i = 1, \ldots, m$, vermöge (24) offenbar wiederum eine Basis von U'.

Satz 17. *Es sei U eine Untergruppe von G mit $\{0\} \subset U \subset G$ (also $n > 1$). Ist $K_1 = r_1 + U, K_2 = r_2 + U, \ldots, K_m = r_m + U$ eine beliebige, aber feste Basis von G/U, wobei die r_i beliebig, aber fest aus den K_i, $i = 1, \ldots, m$, gewählt sein mögen, so stellt jedes System $r_1 + u_1^*, r_2 + u_2^*, \ldots, r_m + u_m^*$ bei beliebiger Wahl der $u_i^* \in U$ jedesmal eine Basis einer Untergruppe U' von G mit $U \dotplus U' = G$ dar. Verschiedene Systeme der u_i^* liefern auch verschiedene U', und auf diese Weise erhält man zu gegebenem U alle möglichen U' mit $U \dotplus U' = G$.*

Beweis. Offenbar gilt $o(K_i) = o(r_i) = p$, $i = 1, \ldots, m$. Angenommen, es sei $\alpha_1(r_1 + u_1^*) + \alpha_2(r_2 + u_2^*) + \cdots + \alpha_m(r_m + u_m^*) = 0$ bei einer beliebigen Wahl der $u_i^* \in U$, und angenommen, es sei hierbei $0 < \alpha_j < p$ für ein bestimmtes α_j. Dann wäre aber $\alpha_1 K_1 + \alpha_2 K_2 + \cdots + \alpha_m K_m = U$ mit $0 < \alpha_j < p$, d. h., die K_i wären linear abhängig und würden also keine Basis von G/U bilden. Es kann also kein $\alpha_j \not\equiv 0 \bmod p$ sein, $i = 1, \ldots, m$. Mithin sind die Elemente $r_i + u_i^*$, $i = 1, \ldots, m$, bei jeder Wahl der $u_i^* \in U$ linear unabhängig. Nun sei U' die von den $r_i + u_i^*$ erzeugte Untergruppe von G, für die die $r_i + u_i^*$ natürlich sogar eine Basis darstellen. Da jedes Element $g \in G$ in einer Klasse G/U liegt und daher in der Form

$$g = u^{**} + [\alpha_1(r_1 + u_1^*) + \cdots + \alpha_m(r_m + u_m^*)] \tag{25}$$

mit passendem $u^{**} \in U$ und passenden ganzen α_i mit $0 \leqq \alpha_i \leqq p-1$, $i = 1, \ldots, m$, darstellbar ist, muß $U + U' = G$ sein. Da außerdem sicherlich $U \cap U' = \{0\}$ gilt, erhält man in der Tat $G = U \dotplus U'$. Nun sei $r_1 + u_1^*, \ldots, r_m + u_m^*$ eine Basis von U' und $r_1 + u_1^{**}, \ldots, r_m + u_m^{**}$ eine Basis von U'' (u_j^*, u_j^{**} aus U). Angenommen, es sei $u_i^* \neq u_i^{**}$, aber $U' = U''$. Dann müßte

$$r_i + u_i^* = \alpha_1(r_1 + u_1^{**}) + \cdots + \alpha_i(r_i + u_i^{**}) + \cdots + \alpha_m(r_m + u_m^{**}) \tag{26}$$

gelten, α_j ganz und $0 \leqq \alpha_j \leqq p-1$, $j = 1, \ldots, m$. Dann wäre aber

$$\begin{aligned} &\alpha_1 r_1 + \cdots + (\alpha_i - 1) r_i + \cdots + \alpha_m r_m \\ &= u_i^* - \alpha_i u_i^{**} - \alpha_1 u_1^{**} - \cdots - \alpha_{i-1} u_{i-1}^{**} - \alpha_{i+1} u_{i+1}^{**} - \cdots - \alpha_m u_m^{**} \end{aligned} \tag{27}$$

und damit ein Element aus U. Da aber die $K_i = r_i + U$, $i = 1, \ldots, m$, eine Basis von G/U darstellen, müßte $\alpha_1 = \alpha_2 = \cdots = \alpha_i - 1 = \cdots = \alpha_m = 0$, also $\alpha_i = 1$ und damit $r_i + u_i^* = r_i + u_i^{**}$, d. h. $u_i^* = u_i^{**}$ gelten. Sind $u_1^*, \ldots, u_m^*$ und $u_1^{**}, \ldots, u_m^{**}$ zwei verschiedene Elementsysteme aus U, so ist also auch $U' \neq U''$. Schließlich folgt aus Satz 16 sofort, daß man auf diese Weise tatsächlich alle möglichen Untergruppen U' mit $U \dotplus U' = G$ erhält. Damit ist Satz 17 vollständig bewiesen.

Zur Aufstellung aller Darstellungen von G als direkte Summe zweier seiner Untergruppen ist nach Satz 17 die Kenntnis einer Basis von G/U erforderlich. Eine solche

läßt sich aber, wie in Satz 18 gezeigt werden soll, bei gegebenem U mit $\{0\} \subset U \subset G$ auf einfache Weise konstruieren. Vorher werde aber noch die folgende Definition aufgestellt.

Definition 6. Ist T eine geordnete, nichttriviale Teilmenge von $\{1, 2, \ldots, n\}$, so werde unter der *Komplementärmenge* S von T die geordnete Menge aller Elemente von $\{1, 2, \ldots, n\}$ verstanden, die nicht zu T gehören.

Satz 18. *Entspricht laut Satz* 14 *der echten Untergruppe U von G die T-Menge $\mathfrak{T}$, zu der gemäß Definition* 5 *die geordnete, nichttriviale Teilmenge $T = \{t_1, t_2, \ldots, t_k\}$ von $\{1, 2, \ldots, n\}$ gehört, und ist $S = \{s_1, s_2, \ldots, s_m\}$, $1 \leqq s_1 < \cdots < s_m \leqq n$, die Komplementärmenge von T, so wird eine Basis von G/U durch die Klassen $r_{s_1} + U, r_{s_2} + U, \ldots, r_{s_m} + U$ gebildet, wobei r_{s_i} von der Form $r_{s_i} = (0, \ldots, 0, k_{s_i}, 0, \ldots, 0)$ ist mit $k_{s_i} = 1$, $i = 1, \ldots, m$.*

Beweis. Sind $b_{t_1}, \ldots, b_{t_k}$ die Elemente von $\mathfrak{T}$, so sind die Elemente $r_{s_1}, \ldots, r_{s_m}$, $b_{t_1}, \ldots, b_{t_k}$ linear unabhängig. Angenommen, es wäre

$$\alpha_1 r_{s_1} + \cdots + \alpha_m r_{s_m} + \beta_1 b_{t_1} + \cdots + \beta_k b_{t_k} = 0, \tag{28}$$

so müßten alle β_ν, $\nu = 1, \ldots, k$, gleich Null sein, denn die Summanden auf der linken Seite von (28) haben z. B. für $\nu = j$ an der Stelle t_j bis auf den Summanden $\beta_j b_{t_j}$ an dieser Stelle alle eine Null stehen, während die t_j-te Stelle von $\beta_j b_{t_j}$ mit β_j besetzt ist. Also ist, da die rechte Seite von (28) gleich Null ist, $\beta_j = 0$. Dies gilt für $j = 1, \ldots, k$. Auf Grund der speziellen Gestalt der r_{s_i} müssen dann aber auch die α_i, $i = 1, \ldots, m$, in (28) gleich Null sein. Also sind $r_{s_1}, \ldots, r_{s_m}, b_{t_1}, \ldots, b_{t_k}$ linear unabhängige Elemente von G, die eine Basis von G darstellen, da $m + k$ gerade gleich der Rang n von G ist. Da aber die b_{t_i} als Elemente von $\mathfrak{T}$ eine Basis von U bilden, erhält man in der Tat durch die Klassen $r_{s_1} + U, r_{s_2} + U, \ldots, r_{s_m} + U$ eine Basis von G/U.

§ 5. Bestimmung der Untergruppenpaare U', U^* von G und der Isomorphismen φ von G/U' auf U^* im Fall $p = 2$

Zur Konstruktion der Automorphismen der Ordnung 2 einer endlichen elementaren abelschen Gruppe G vom Rang $n \geqq 1$ für die Primzahl $p = 2$ müssen nach Satz 10 alle Untergruppenpaare U', U^* von G mit $\{0\} \subset U'$, $U^* \subseteqq U'$, $o(U^*) \cdot o(U') = o(G)$ und alle Isomorphismen φ von G/U' auf U^* bestimmt werden.

1. Die Bestimmung der Untergruppenpaare U', U^* von G

Ist $U' = G$, so erhält man für U^* nur die Untergruppe $U^* = \{0\}$, was den trivialen Fall des identischen Automorphismus $\sigma = \varepsilon$ von G ergibt. Deshalb kann im folgenden $U' \subset G$ vorausgesetzt werden. Ferner kann auch $n \geqq 2$ angenommen werden, da im Fall $n = 1$ auf Grund von $\{0\} \subset U'$ nur $U' = G$ möglich ist. Wegen $\{0\} \subset U'$, $U^* \subseteqq U' \subset G$ und $o(U^*) \cdot o(U') = o(G) = 2^n$ muß für $o(U')$ und $o(U^*)$

$$o(U') = 2^\nu \quad \text{mit} \quad \frac{n}{2} + \left(\frac{1}{4} + (-1)^{n+1}\frac{1}{4}\right) \leqq \nu \leqq n - 1, \tag{29}$$

$$o(U^*) = \frac{o(G)}{o(U')} = 2^{n-\nu} \tag{30}$$

gelten. Die Untergruppen U' lassen sich nach Wahl einer festen Basis $a_1, \ldots, a_n$ von G gemäß § 3 bestimmen, man braucht nur sämtliche T-Mengen zu konstruieren, die zu den geordneten Teilmengen $\{t_1, t_2, \ldots, t_\nu\}$ von $\{1, 2, \ldots, n\}$ gehören, wobei ν alle ganzen Zahlen durchläuft, die den Ungleichungen in (29) genügen. Ist nun U' eine solche nach § 3 konstruierte Untergruppe von G der Ordnung $o(U') = 2^\nu$, wobei ν den Ungleichungen in (29) genügt, und sind $b_1, \ldots, b_\nu$ die Elemente der zu U' gehörenden T-Menge, so lassen sich die Untergruppen U^* von U' wieder gemäß § 3 bestimmen, wobei man die Elemente

$$b_1, \ldots, b_\nu \tag{31}$$

als Basiselemente von U' wählt und jetzt sämtliche T-Mengen konstruiert, die zu den geordneten Teilmengen $\{t_1^*, t_2^*, \ldots, t_{n-\nu}^*\}$ von $\{1, 2, \ldots, \nu\}$ gehören. Die Elemente dieser T-Mengen sollen dann mit

$$c_1, \ldots, c_{n-\nu} \tag{32}$$

bezeichnet werden. Sie stellen natürlich eine Basis von U^* dar und sind Linearkombinationen aus den Elementen (31), lassen sich selbstverständlich aber auch aus den Basiselementen a_k, $k = 1, \ldots, n$, von G linear kombinieren.

2. Bestimmung der Isomorphismen φ von G/U auf U^*

Nach Satz 18 läßt sich, falls U' eine echte Untergruppe von G ist, die spezielle Basis $K_1 = r_{s_1} + U', \ldots, K_{n-\nu} = r_{s_{n-\nu}} + U'$ von G/U' konstruieren. Sind $c_1, \ldots, c_{n-\nu}$ die Basiselemente (32) von U^*, so ist dann offenbar durch

$$\varphi^*(K_i) = c_i, \quad i = 1, \ldots, n - \nu, \tag{33}$$

ein Isomorphismus φ^* von G/U' auf U^* gegeben. Ist jetzt $\tilde{\varphi}$ ein Automorphismus von U^*, so wird durch

$$\tilde{\varphi}\big(\varphi^*(K_i)\big) = \tilde{\varphi}(c_i) = \varphi(K_i) \tag{34}$$

gleichfalls ein Isomorphismus φ von G/U' auf U^* vermittelt, und zwei verschiedene Automorphismen $\tilde{\varphi}_1$, $\tilde{\varphi}_2$ von U^* liefern offenbar auch zwei verschiedene Isomorphismen φ_1, φ_2 von G/U' auf U^*. Ist umgekehrt φ' ein beliebiger Isomorphismus von G/U' auf U^*, so gilt $\varphi'(K_i) = d_i$, $i = 1, \ldots, n - \nu$, und die d_i bilden eine Basis von U^*. Dann gibt es aber einen Automorphismus $\bar{\varphi}$ von U^* mit $\bar{\varphi}(c_i) = d_i$ und $\varphi'(K_i) = \bar{\varphi}(c_i) = \bar{\varphi}\big(\varphi^*(K_i)\big)$. Man kann also sämtliche Isomorphismen von G/U' auf U^* angeben, wenn man alle Automorphismen von U^* konstruieren kann. Dies ist aber nach einer früheren Arbeit ([2], S. 113) möglich und läßt sich wie folgt durchführen:
Es sei

$$\mathfrak{A}_{n-\nu} = \begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1,n-\nu} \\ \vdots & & \vdots \\ \gamma_{n-\nu,1} & \cdots & \gamma_{n-\nu,n-\nu} \end{pmatrix} \tag{35}$$

die einen Automorphismus γ von U^* vermittelnde Matrix vermöge

$$\begin{pmatrix} \gamma(c_1) \\ \vdots \\ \gamma(c_{n-\nu}) \end{pmatrix} = \mathfrak{A}_{n-\nu} \begin{pmatrix} c_1 \\ \vdots \\ c_{n-\nu} \end{pmatrix}. \tag{36}$$

Die Matrix $\mathfrak{A}_{n-\nu}$ erhält man nun durch das folgende Verfahren: Zunächst wird eine

Matrix $\mathfrak{A}^*_{n-\nu}$ aufgestellt, bei der man die Elemente der ersten Zeile beliebig 1 oder 0 setzt, wobei aber mindestens einmal eine 1 vorkommen muß. Steht im Fall $n - \nu > 1$ in der ersten Zeile von $\mathfrak{A}^*_{n-\nu}$ zum erstenmal an der Stelle $\gamma_{1\mu}$ eine 1, so werden die restlichen Elemente der μ-ten Spalte mit lauter Nullen belegt. Entsprechend wird dann fortlaufend mit den übrigen Zeilen verfahren. Anschließend kann dann noch die so gewonnene Matrix $\mathfrak{A}^*_{n-\nu}$ von links mit einer Matrix $\mathfrak{D}_{n-\nu}$ der Form

$$\mathfrak{D}_{n-\nu} = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & \ddots & \\ \lambda & & 1 \end{pmatrix} \tag{37}$$

multipliziert werden, wobei an den Stellen unterhalb der Hauptdiagonale beliebig die Zahlen 0 oder 1 gesetzt werden können. Das Produkt $\mathfrak{D}_{n-\nu}\mathfrak{A}^*_{n-\nu}$ liefert dann stets eine Matrix $\mathfrak{A}_{n-\nu}$, die einen Automorphismus γ von U^* vermittelt, und auf diese Weise erhält man alle Automorphismen von U^*.

Beispiel. $p = 2$, $n - \nu = 4$.

$$\mathfrak{A}^*_4 = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \gamma_{13} & \gamma_{14} \\ \gamma_{21} & \gamma_{22} & \gamma_{23} & \gamma_{24} \\ \gamma_{31} & \gamma_{32} & \gamma_{33} & \gamma_{34} \\ \gamma_{41} & \gamma_{42} & \gamma_{43} & \gamma_{44} \end{pmatrix}. \quad \text{1. Schritt:} \begin{pmatrix} 0 & 1 & 1 & 0 \\ & 0 & & \\ & 0 & & \\ & 0 & & \end{pmatrix}, \quad \text{2. Schritt:} \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ & & 0 & 0 \\ & & 0 & 0 \end{pmatrix},$$

$$\text{3. Schritt:} \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & \end{pmatrix}, \quad \text{4. Schritt:} \ \mathfrak{A}^*_4 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$\mathfrak{D}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix};$$

$$\mathfrak{A}_4 = \mathfrak{D}_4\mathfrak{A}^*_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

(Alle Rechnungen wurden natürlich mod 2 durchgeführt.)

§ 6. Konstruktion der Automorphismen der Ordnung 2 von G im Fall $p \neq 2$

Nach den vorangegangenen Paragraphen ist es nun nicht mehr schwer, alle Automorphismen der Ordnung 2 von G zu konstruieren. Im Fall $p \neq 2$ braucht G nach Satz 4 nur in der Form $G = U + U'$ dargestellt zu werden. Dabei kann man nach Satz 15 von einer beliebigen Untergruppe U von G ausgehen. Wie man jede Untergruppe U von G bestimmen kann, wurde in § 3 gezeigt. In § 4 wurde schließlich dargelegt, wie zu gegebenem U alle Untergruppen U' mit $U + U' = G$ erhalten werden

können. Ist dann $c_1, \ldots, c_r$ eine Basis von U und $d_1, \ldots, d_s$ eine Basis von U', so wird durch $\sigma(c_i) = c_i$, $i = 1, \ldots, r$, und $\sigma(d_j) = -d_j = (p-1)\,d_j$, $j = 1, \ldots, s$, ein Automorphismus σ der Ordnung 2 von G festgelegt. Auf diese Weise erhält man auch alle Automorphismen σ der Ordnung 2 von G.

Es sei also G eine endliche elementare abelsche Gruppe vom Rang $n \geqq 1$ und vom Typus $(p, p, \ldots, p)$, wobei p eine Primzahl ungleich 2 sein soll. Ferner möge $a_1, \ldots, a_n$ eine feste Basis von G sein, die dann nach (6) wie folgt dargestellt werden kann: $a_1 = (1, 0, \ldots, 0)$, $a_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $a_n = (0, \ldots, 0, 1)$.

Die Konstruktion der Automorphismen σ der Ordnung 2 von G läßt sich nun in folgenden Schritten durchführen:

1. Ist der Rang n von G gleich 1, so ist $G = \{0\} + \{a_1\}$ oder $G = \{a_1\} + \{0\}$, $a_1 \neq 0$ beliebig aus G. Im ersten Fall ist $\sigma(a_1) = -a_1 = (p-1)\,a_1$, und im zweiten Fall gilt $\sigma(a_1) = a_1$. Die diese Automorphismen vermittelnden Matrizen $\mathfrak{A}_1$ lauten dann $\mathfrak{A}_1 = (p-1)$ bzw. $\mathfrak{A}_1 = (1)$. Der erste Automorphismus ist der Automorphismus τ aus Bemerkung 1 und der zweite ist der identische Automorphismus ε.

2. Im Fall $n > 1$ wähle man eine beliebige geordnete nichttriviale Teilmenge T von $\{1, 2, \ldots, n\}$: $T = \{t_1, t_2, \ldots, t_k\}$, $1 \leqq t_1 < t_2 < \cdots < t_k \leqq n$.

3. Dann wird zu T eine beliebige zugehörige T-Menge $\mathfrak{T}$ gebildet: $B_1 = b_{t_1}, \ldots, B_k = b_{t_k}$ mit $b_{t_i} = (0, \ldots, 0, 1, \ldots)$, $i = 1, \ldots, k$. Die 1 steht an der t_i-ten Stelle. Links von der 1 stehen (falls $t_i > 1$ ist) lauter Nullen. An allen Stellen $t_j \in T$ mit $t_j > t_i$ (falls solche Stellen vorhanden sind) wird eine Null gesetzt, und alle übrigen Stellen $t_l > t_i$ werden (falls solche vorhanden sind) beliebig mit ganzen Zahlen z_l mit $0 \leqq z_l \leqq p-1$ belegt.

4. Es wird dann $U = \{B_1, \ldots, B_k\}$ gesetzt.

5. Man bildet als nächstes die Komplementärmenge $S = \{s_1, s_2, \ldots, s_m\}$, $1 \leqq s_1 < s_2 < \cdots < s_m \leqq n$, von T gemäß Definition 6.

6. Zu S werden die Elemente $r_{s_1}, \ldots, r_{s_m}$ mit $r_{s_i} = (0, \ldots, 0, 1, 0, \ldots, 0)$ aufgestellt, wobei die 1 an der Stelle s_i steht und alle anderen Stellen mit Nullen belegt werden.

7. Zu jedem r_{s_i} wird beliebig ein $u_i^* \in U$, $i = 1, \ldots, m$, gewählt.

8. Es wird dann $U' = \{r_{s_1} + u_1^*, \ldots, r_{s_m} + u_m^*\}$ gesetzt.

9. Durch $\sigma(B_i) = B_i$, $i = 1, \ldots, k$, und $\sigma(r_{s_j} + u_j^*) = (p-1)\,(r_{s_j} + u_j^*)$, $j = 1, \ldots, m$, ist dann ein Automorphismus σ der Ordnung 2 von G gegeben.

10. Hat man auf diese Weise ein σ konstruiert, so kann man noch die den Automorphismus σ vermittelnde Matrix

$$\mathfrak{A}_n = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{pmatrix}$$

bezüglich der Basis $a_1, \ldots, a_n$ von G auf folgende Weise aufstellen: Es ist

$$\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} B_1 \\ \vdots \\ B_k \\ r_{s_1} + u_1^* \\ \vdots \\ r_{s_m} + u_m^* \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}. \tag{38}$$

Auf Grund der Hilfssätze 1 und 2 läßt sich durch passende Zeilenumformungen erreichen, daß (38) in

$$\begin{pmatrix} b_{11} \dots b_{1n} \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ b_{n1} \dots b_{nn} \end{pmatrix} \begin{pmatrix} B_1 \\ \vdots \\ B_k \\ r_{s_1} + u_1^* \\ \vdots \\ r_{s_m} + u_m^* \end{pmatrix} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & & & & \\ \cdot & & \cdot & & & \\ \cdot & & & \cdot & & \\ \cdot & & & & \cdot & \\ 0 & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{pmatrix} \tag{39}$$

übergeht, also

$$\left(\begin{array}{cccc|ccc} 1 & \cdot & \cdot & 0 & a_{11} & \dots & a_{1n} \\ \cdot & \cdot & & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & \cdot & & \cdot \\ 0 & \cdot & \cdot & 1 & a_{n1} & \dots & a_{nn} \end{array}\right) \to \left(\begin{array}{ccc|ccc} b_{11} & \dots & b_{1n} & 1 & \cdot & 0 \\ \cdot & & \cdot & \cdot & \cdot & \cdot \\ \cdot & & \cdot & \cdot & \cdot & \cdot \\ b_{n1} & \dots & b_{nn} & 0 & \cdot & 1 \end{array}\right)$$

durch passende Zeilenumformungen nach Hilfssatz 1 und Hilfssatz 2. Nun ist

$$\begin{pmatrix} \sigma(B_1) \\ \vdots \\ \sigma(B_k) \\ \sigma(r_{s_1} + u_1^*) \\ \vdots \\ \sigma(r_{s_m} + u_m^*) \end{pmatrix} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & & & & & & \cdot \\ \cdot & & \cdot & & & & & & \cdot \\ \cdot & & & 1 & & & & & \cdot \\ \cdot & & & & p-1 & & & & \cdot \\ \cdot & & & & & \cdot & & & \cdot \\ \cdot & & & & & & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & p-1 \end{pmatrix} \begin{pmatrix} B_1 \\ \vdots \\ B_k \\ r_{s_1} + u_1^* \\ \vdots \\ r_{s_m} + u_m^* \end{pmatrix} \tag{40}$$

(k Einsen in der Hauptdiagonalen der ersten Matrix rechts) und hierin (38) eingesetzt ergibt

$$\begin{pmatrix} (\sigma B_1) \\ \vdots \\ \sigma(B_k) \\ \sigma(r_{s_1} + u_1^*) \\ \vdots \\ \sigma(r_{s_m} + u_m^*) \end{pmatrix} = \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & & & & & & \cdot \\ \cdot & & \cdot & & & & & & \cdot \\ \cdot & & & 1 & & & & & \cdot \\ \cdot & & & & p-1 & & & & \cdot \\ \cdot & & & & & \cdot & & & \cdot \\ \cdot & & & & & & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & p-1 \end{pmatrix} \begin{pmatrix} a_{11} \dots a_{1n} \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ a_{n1} \dots a_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{pmatrix}. \tag{41}$$

σ auf (39) angewendet ergibt schließlich unter Berücksichtigung von (41):

$$\begin{pmatrix} \sigma(a_1) \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \sigma(a_n) \end{pmatrix} = \begin{pmatrix} b_{11} \dots b_{1n} \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ b_{n1} \dots b_{nn} \end{pmatrix} \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & & & & & & \cdot \\ \cdot & & \cdot & & & & & & \cdot \\ \cdot & & & 1 & & & & & \cdot \\ \cdot & & & & p-1 & & & & \cdot \\ \cdot & & & & & \cdot & & & \cdot \\ \cdot & & & & & & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & p-1 \end{pmatrix} \begin{pmatrix} a_{11} \dots a_{1n} \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ a_{n1} \dots a_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{pmatrix} \tag{42}$$

also

$$\mathfrak{A}_n = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{pmatrix},$$

$$= \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & p-1 & & & \\ & & & & \ddots & & \\ 0 & & & & & & p-1 \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}. \quad (43)$$

11. Wählt man $T = \{1, 2, \ldots, n\}$, so ist $U = G$ und damit $G = G \dotplus \{0\}$, was dem identischen Automorphismus $\sigma = \varepsilon$ der Ordnung 2 von G mit $\varepsilon(a) = a$ für alle $a \in G$ entspricht. Wählt man $T = \emptyset$, so werde $U = \{0\}$ gesetzt. Also ist dann $G = \{0\} \dotplus G$, was dem Automorphismus $\sigma = \tau$ der Ordnung 2 von G mit $\tau(b) = -b = (p-1)\,b$ für alle $b \in G$ entspricht. [Zum Punkt 11 siehe auch die Bemerkung 1.]

Beispiel. G sei vom Typus (3, 3, 3, 3), und a_1, a_2, a_3, a_4 sei eine feste Basis von G. Der Rang n von G ist also gleich 4, d. h. größer als 1, mithin kann gleich bei Punkt 2 begonnen werden:

2. Es werde $T = \{2\}$, d. h. $T = \{t_1\}$ mit $t_1 = 2$ gewählt. (Also ist $k = 1$.)

3. Es sei $B_1 = b_{t_1} = b_2 = (0, 1, 2, 1)$.

4. $U = \{(0, 1, 2, 1)\}$.

5. $S = \{s_1, s_2, s_3\} = \{1, 3, 4\}$. (Also ist $m = 3$.)

6. $r_{s_1} = (1, 0, 0, 0)$, $r_{s_2} = (0, 0, 1, 0)$, $r_{s_3} = (0, 0, 0, 1)$.

7. Es sei $u_1^* = (0, 1, 2, 1)$, $u_2^* = (0, 1, 2, 1)$, $u_3^* = (0, 2, 1, 2)$.

8. $U' = \{r_{s_1} + u_1^*, r_{s_2} + u_2^*, r_{s_3} + u_3^*\} = \{(1, 1, 2, 1), (0, 1, 0, 1), (0, 2, 1, 0)\}$.

9. $\sigma[(0, 1, 2, 1)] = (0, 1, 2, 1)$, $\sigma[(1, 1, 2, 1)] = (2, 2, 1, 2)$,
$\sigma[(0, 1, 0, 1)] = (0, 2, 0, 2)$, $\sigma[(0, 2, 1, 0)] = (0, 1, 2, 0)$.

10. $$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 \end{pmatrix},$$

also

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & 0 \end{array}\right) \to \left(\begin{array}{cccc|cccc} 0 & 1 & 0 & 0 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & 0 \end{array}\right)$$

$$\to\left(\begin{array}{cccc|cccc} 0 & 1 & 2 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 & 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{cccc|cccc} 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 2 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right),$$

mithin

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 2 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Damit ergibt sich nach (43)

$$\mathfrak{A}_4 = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 2 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 \end{pmatrix},$$

d. h.

$$\mathfrak{A}_4 = \begin{pmatrix} 2 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 \end{pmatrix}.$$

In der Tat ist auch $\mathfrak{A}_4^2 \equiv \mathfrak{E}_4 \bmod 3$. (Alle Rechnungen wurden natürlich mod 3 durchgeführt.) Mit $\mathfrak{A}_4$ ergibt sich dann der folgende Automorphismus σ der Ordnung 2 von G:

$$\begin{aligned} \sigma(a_1) &= 2a_1 + a_2 + 2a_3 + a_4, \\ \sigma(a_2) &= 2a_3 + a_4, \\ \sigma(a_3) &= a_2 + a_3 + a_4, \\ \sigma(a_4) &= 2a_2 + a_3 + a_4. \end{aligned}$$

§ 7. Konstruktion der Automorphismen der Ordnung 2 von G im Fall $p = 2$

Ebenso wie im Fall $p \neq 2$ ist es nun auch im Fall $p = 2$ nicht mehr schwer, alle Automorphismen der Ordnung 2 von G zu konstruieren. Nach Satz 10 kann man von einer beliebigen Untergruppe U' von G ausgehen, wobei aber, falls nicht $U' = G$ ist, (29) berücksichtigt werden muß. Diese Untergruppen lassen sich nach § 3 bestimmen. Ebenso lassen sich dann nach § 3 alle Untergruppen U^* von U' angeben, für die $o(U^*) \cdot o(U') = o(G)$ gilt. Nach den Ausführungen des § 5, Abschnitt 2, ist es auch einfach, alle Isomorphismen φ von G/U' auf U^* anzugeben. Ein Automorphismus σ der Ordnung 2 von G wird dann durch $\sigma(g) = g + \varphi(K(g))$, $g \in G$, festgelegt, wobei mit $K(g)$ die Klasse von G/U' bezeichnet wird, in der das Element $g \in G$ liegt. Auf diese Weise erhält man auch alle Automorphismen σ der Ordnung 2 von G.

Es sei also G eine endliche elementare abelsche Gruppe vom Rang $n \geqq 1$ und vom Typus $(2, 2, \ldots, 2)$. Ferner möge $a_1, \ldots, a_n$ eine feste Basis von G sein, die dann nach

(6) wie folgt dargestellt werden kann: $a_1 = (1, 0, \ldots, 0)$, $a_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $a_n = (0, \ldots, 0, 1)$. Die Konstruktion der Automorphismen σ der Ordnung 2 von G läßt sich nun in folgenden Schritten durchführen.

1. Ist der Rang n von G gleich 1, so besteht G nur aus den Elementen 0 und a mit $2a = 0$, und der einzige Automorphismus von G, der überhaupt existiert, ist der identische Automorphismus $\sigma = \varepsilon$ mit $\varepsilon(0) = 0$, $\varepsilon(a) = a$, der natürlich auch als ein Automorphismus der Ordnung 2 aufgefaßt werden kann.

2. Ist der Rang n von G größer gleich 2 und wählt man U' mit $o(U') = 2^r = 2^n$, also $U' = G$, so existiert in diesem Fall als einziger Automorphismus der Ordnung 2 auch nur der identische Automorphismus $\sigma = \varepsilon$ von G, weil dann nach Satz 10 gerade $\sigma(a) = a$ für alle $a \in G$ gilt, also $\sigma = \varepsilon$ ist.

3. Es sei nun $n \geqq 2$ und $o(U') = 2^r \neq 2^n$. Man wähle dann ν beliebig, aber so, daß $\frac{n}{2} + \left(\frac{1}{4} + (-1)^{n+1}\frac{1}{4}\right) \leqq \nu \leqq n - 1$ gilt.

4. T_1 sei dann eine beliebige geordnete Teilmenge $T_1 = \{t_1, t_2, \ldots, t_\nu\}$, $1 \leqq t_1 < t_2 < \cdots < t_\nu \leqq n$, von $\{1, 2, \ldots, n\}$.

5. Dann wird zu T_1 eine beliebige zugehörige T-Menge $\mathfrak{T}_1$ (bezüglich der Basis $a_1, \ldots, a_n$) gebildet: $B_1 = b_{t_1}, \ldots, B_\nu = b_{t_\nu}$ mit $b_{t_i} = (0, \ldots, 0, 1, \ldots)$, $i = 1, \ldots, \nu$. Die 1 steht an der t_i-ten Stelle, links von der 1 stehen (falls $t_i > 1$ ist) lauter Nullen. An allen Stellen $t_j \in T$ mit $t_j > t_i$ wird (falls solche Stellen vorhanden sind) eine Null gesetzt, und alle übrigen Stellen $t_l > t_j$ werden (falls solche vorhanden sind) beliebig mit 0 oder mit 1 belegt.

6. Es wird dann $U' = \{B_1, \ldots, B_\nu\}$ gesetzt, und es ist

$$\begin{pmatrix} B_1 \\ \vdots \\ B_\nu \end{pmatrix} = \begin{pmatrix} \alpha_{11} \ldots \alpha_{1n} \\ \vdots \quad\quad \vdots \\ \alpha_{\nu 1} \ldots \alpha_{\nu n} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \mathfrak{A}_{\nu,n} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}. \tag{44}$$

7. Weiter sei T_2 eine beliebige geordnete Teilmenge $T_2 = \{j_1, j_2, \ldots, j_{n-\nu}\}$, $1 \leqq j_1 < j_2 < \cdots < j_{n-\nu} \leqq \nu$, aus $n - \nu$ Elementen von $\{1, 2, \ldots, \nu\}$.

8. Dann wird zu T_2 eine beliebige zugehörige T-Menge $\mathfrak{T}_2$ (bezüglich der Basis $B_1, \ldots, B_\nu$) aufgestellt: $C_1 = c_{j_1}, \ldots, C_{n-\nu} = c_{j_{n-\nu}}$, wobei die c_{j_i}, $i = 1, \ldots, n - \nu$, genau so wie die b_{t_i} unter 5. gebildet werden.

9. Es wird dann $U^* = \{C_1, \ldots, C_{n-\nu}\}$ gesetzt, und es ist

$$\begin{pmatrix} C_1 \\ \vdots \\ C_{n-\nu} \end{pmatrix} = \begin{pmatrix} \beta_{11} \quad \cdots \quad \beta_{1\nu} \\ \vdots \quad\quad\quad \vdots \\ \beta_{n-\nu,1} \cdots \beta_{n-\nu,\nu} \end{pmatrix} \begin{pmatrix} B_1 \\ \vdots \\ B_\nu \end{pmatrix} = \mathfrak{B}_{n-\nu,\nu} \begin{pmatrix} B_1 \\ \vdots \\ B_\nu \end{pmatrix}. \tag{45}$$

10. Es sei jetzt S_1 die Komplementärmenge von T_1, also $S_1 = \{s_1, s_2, \ldots, s_{n-\nu}\}$, $1 \leqq s_1 < s_2 < \cdots < s_{n-\nu} \leqq n$. Nach Satz 18 wird nun die spezielle Basis $K_1 = r_{s_1} + U', \ldots, K_{n-\nu} = r_{s_{n-\nu}} + U'$ mit $r_{s_i} = (0, \ldots, 0, 1, 0, \ldots, 0)$, $i = 1, \ldots, n - \nu$, die 1 steht an der Stelle s_i, von G/U' aufgestellt, und durch $\varphi^*(K_i) = C_i$, $i = 1, \ldots, n - \nu$, ist dann ein bestimmter Isomorphismus von G/U' auf U^* festgelegt.

11. Nun wird ein beliebiger Automorphismus $\tilde{\varphi}$ von U^* nach der Vorschrift aus § 5, Abschnitt 2, konstruiert, und es sei

$$\mathfrak{C}_{n-\nu} = \begin{pmatrix} \gamma_{11} \quad \cdots \quad \gamma_{1,n-\nu} \\ \vdots \quad\quad\quad \vdots \\ \gamma_{n-\nu,1} \cdots \gamma_{n-\nu,n-\nu} \end{pmatrix} \tag{46}$$

die diesen Automorphismus vermittelnde Matrix.

12. Man bildet dann den Isomorphismus $\varphi(K_i) = \tilde{\varphi}(C_i) = \tilde{\varphi}(\varphi^*(K_i))$.

13. Durch $\sigma(g) = g + \varphi(K(g))$, $g \in G$, $K(g)$ Klasse von G/U', in der g liegt, ist dann ein Automorphismus σ der Ordnung 2 von G gegeben.

14. σ kann auch durch eine Matrix $\mathfrak{A}_n^*$ bezüglich einer festen Basis von G angegeben werden. Als Basis von G lassen sich offenbar die Elemente $B_1, \ldots, B_\nu, r_{s_1}, \ldots, r_{s_{n-\nu}}$ wählen. Dann ist aber $\sigma(B_i) = B_i + 0$ für $i = 1, \ldots, \nu$, da $B_i \in U'$ und $\varphi(U') = 0$ ist. Liegt r_{s_j} in der Klasse K_j von G/U', so gilt

$$\sigma(r_{s_j}) = r_{s_j} + \varphi(K_j) = r_{s_j} + \tilde{\varphi}(C_j) = r_{s_j} + \gamma_{j1}C_1 + \cdots + \gamma_{j,n-\nu}C_{n-\nu},$$

$j = 1, \ldots, n - \nu$, also

$$\begin{pmatrix} \sigma(r_{s_1}) \\ \vdots \\ \sigma(r_{s_{n-\nu}}) \end{pmatrix} = \begin{pmatrix} r_{s_1} \\ \vdots \\ r_{s_{n-\nu}} \end{pmatrix} + \begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1,n-\nu} \\ \vdots & & \vdots \\ \gamma_{n-\nu,1} & \cdots & \gamma_{n-\nu,n-\nu} \end{pmatrix} \begin{pmatrix} C_1 \\ \vdots \\ C_{n-\nu} \end{pmatrix}. \tag{47}$$

Wird hierin (45) eingesetzt, so ergibt sich

$$\begin{pmatrix} \sigma(r_{s_1}) \\ \vdots \\ \sigma(r_{s_{n-\nu}}) \end{pmatrix} = \begin{pmatrix} r_{s_1} \\ \vdots \\ r_{s_{n-\nu}} \end{pmatrix} + \begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1,n-\nu} \\ \vdots & & \vdots \\ \gamma_{n-\nu,1} & \cdots & \gamma_{n-\nu,n-\nu} \end{pmatrix} \begin{pmatrix} \beta_{11} & \cdots & \beta_{1\nu} \\ \vdots & & \vdots \\ \beta_{n-\nu,1} & \cdots & \beta_{n-\nu,\nu} \end{pmatrix} \begin{pmatrix} B_1 \\ \vdots \\ B_\nu \end{pmatrix} \tag{48}$$

oder

$$\begin{pmatrix} \sigma(r_{s_1}) \\ \vdots \\ \sigma(r_{s_{n-\nu}}) \end{pmatrix} = \mathfrak{D}_{n-\nu,\nu} \begin{pmatrix} B_1 \\ \vdots \\ B_\nu \end{pmatrix} + \begin{pmatrix} r_{s_1} \\ \vdots \\ r_{s_{n-\nu}} \end{pmatrix} \tag{49}$$

mit

$$\mathfrak{D}_{n-\nu,\nu} = \mathfrak{C}_{n-\nu}\mathfrak{B}_{n-\nu,\nu}. \tag{50}$$

Damit erhält man schließlich

$$\begin{pmatrix} \sigma(B_1) \\ \vdots \\ \sigma(B_\nu) \\ \sigma(r_{s_1}) \\ \vdots \\ \sigma(r_{s_{n-\nu}}) \end{pmatrix} = \begin{pmatrix} \mathfrak{E}_\nu & 0 \\ \mathfrak{D}_{n-\nu,\nu} & \mathfrak{E}_{n-\nu} \end{pmatrix} \begin{pmatrix} B_1 \\ \vdots \\ B_\nu \\ r_{s_1} \\ \vdots \\ r_{s_{n-\nu}} \end{pmatrix} = \mathfrak{A}_n^* \begin{pmatrix} B_1 \\ \vdots \\ B_\nu \\ r_{s_1} \\ \vdots \\ r_{s_{n-\nu}} \end{pmatrix}, \tag{51}$$

wobei

$$\mathfrak{A}_n^* = \begin{pmatrix} \mathfrak{E}_\nu & 0 \\ \mathfrak{D}_{n-\nu,\nu} & \mathfrak{E}_{n-\nu} \end{pmatrix} \tag{52}$$

gesetzt wurde.

15. Nun sei $\mathfrak{M}_n$ die Matrix, die den Übergang von der Basis $a_1, \ldots, a_n$ zu der Basis $B_1, \ldots, B_\nu, r_{s_1}, \ldots, r_{s_{n-\nu}}$ vermittelt, also

$$\begin{pmatrix} B_1 \\ \vdots \\ B_\nu \\ r_{s_1} \\ \vdots \\ r_{s_{n-\nu}} \end{pmatrix} = \mathfrak{M}_n \begin{pmatrix} a_1 \\ \vdots \\ a_\nu \\ a_{\nu+1} \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \alpha_{11} \cdots \alpha_{1n} \\ \vdots \\ \alpha_{\nu 1} \cdots \alpha_{\nu n} \\ 0 \ldots 1 \ldots 0 \\ \vdots \\ 0 \ldots 1 \ldots 0 \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_\nu \\ a_{\nu+1} \\ \vdots \\ a_n \end{pmatrix}. \tag{53}$$

Hierin sind die α_{ij} die Elemente aus $\mathfrak{A}_{\nu,n}$ in (44). In der $(\nu+1)$-ten Zeile von $\mathfrak{M}_n$ steht an der s_1-ten Stelle eine 1, in der $(\nu+2)$-ten Zeile an der s_2-ten Stelle eine 1 usw., schließlich in der n-ten Zeile an der $s_{n-\nu}$-ten Stelle eine 1, während alle anderen Stellen in der $(\nu+1)$-ten bis n-ten Zeile mit 0 belegt sind. Da $\mathfrak{M}_n$ den Übergang von einer Basis zu einer anderen vermittelt, existiert auch zu $\mathfrak{M}_n$ die Matrix $\mathfrak{M}_n^{-1}$ mit $\mathfrak{M}_n^{-1}\mathfrak{M}_n = \mathfrak{E}_n$, und damit erhält man aus (53) sofort

$$\begin{pmatrix} a_1 \\ \vdots \\ a_\nu \\ a_{\nu+1} \\ \vdots \\ a_n \end{pmatrix} = \mathfrak{M}_n^{-1} \begin{pmatrix} B_1 \\ \vdots \\ B_\nu \\ r_{s_1} \\ \vdots \\ r_{s_{n-\nu}} \end{pmatrix}. \tag{54}$$

Verwendet man (51) und nochmals (53), so ergibt sich aus (54) schließlich

$$\begin{pmatrix} \sigma(a_1) \\ \vdots \\ \sigma(a_\nu) \\ \sigma(a_{\nu+1}) \\ \vdots \\ \sigma(a_n) \end{pmatrix} = \mathfrak{M}_n^{-1}\mathfrak{A}_n^*\mathfrak{M}_n \begin{pmatrix} a_1 \\ \vdots \\ a_\nu \\ a_{\nu+1} \\ \vdots \\ a_n \end{pmatrix} \tag{55}$$

mit

$$\mathfrak{A}_n = \mathfrak{M}_n^{-1}\mathfrak{A}_n^*\mathfrak{M}_n \tag{56}$$

als der den Automorphismus σ vermittelnden Matrix bezüglich der Basis $a_1, \ldots, a_n$.

Beispiel. G sei vom Typus (2, 2, 2, 2, 2, 2, 2), und $a_1, a_2, a_3, a_4, a_5, a_6, a_7$ sei eine feste Basis von G. Der Rang n von G ist also gleich 7, d. h. größer als 2, mithin kann gleich bei Punkt 2 bzw. bei Punkt 3 begonnen werden. Wird mit Punkt 3 angefangen, so muß zunächst ein ν mit $\frac{7}{2} + \left(\frac{1}{4} + (-1)^{n+1}\frac{1}{4}\right) \leqq \nu \leqq 7 - 1$, d. h. mit $4 \leqq \nu \leqq 6$ gewählt werden. Es sei z. B. $\nu = 5$ und damit $n - \nu = 2$. Weiter sei dann

4. $T_1 = \{t_1, t_2, t_3, t_4, t_5\} = \{2, 3, 4, 5, 7\}$, also $t_1 = 2$, $t_2 = 3$, $t_3 = 4$, $t_4 = 5$, $t_5 = 7$.
5. Es sei

$$\begin{aligned} B_1 &= b_{t_1} = b_2 = (0, 1, 0, 0, 0, 1, 0), \\ B_2 &= b_{t_2} = b_3 = (0, 0, 1, 0, 0, 1, 0), \\ B_3 &= b_{t_3} = b_4 = (0, 0, 0, 1, 0, 0, 0), \\ B_4 &= b_{t_4} = b_5 = (0, 0, 0, 0, 1, 1, 0), \\ B_5 &= b_{t_5} = b_7 = (0, 0, 0, 0, 0, 0, 1). \end{aligned}$$

6. $U' = \{B_1, B_2, B_3, B_4, B_5\}$.

$$\begin{pmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \end{pmatrix} = \mathfrak{A}_{5,7} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix}, \quad \mathfrak{A}_{5,7} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Weiter sei

7. $T_2 = \{j_1, j_2\} = \{3, 4\}$, also $j_1 = 3$, $j_2 = 4$.
8. Es sei $C_1 = c_{j_1} = c_3 = (0, 0, 1, 0, 1)$, $C_2 = c_{j_2} = c_4 = (0, 0, 0, 1, 1)$.
9. $U^* = \{C_1, C_2\}$,

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \mathfrak{B}_{2,5} \begin{pmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \end{pmatrix}, \qquad \mathfrak{B}_{2,5} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

10. $S_1 = \{s_1, s_2\} = \{1, 6\}$, also $s_1 = 1$, $s_2 = 6$.
$K_1 = (1, 0, 0, 0, 0, 0, 0) + U'$, $K_2 = (0, 0, 0, 0, 0, 1, 0) + U'$.
$\varphi^*(K_1) = C_1$, $\varphi^*(K_2) = C_2$.
11. Es sei nun nach § 5, Abschnitt 2, z. B.

$$\mathfrak{C}_2 = \mathfrak{D}\mathfrak{A}^* = \begin{pmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

12. $\varphi(K_1) = \tilde{\varphi}(C_1) = C_1 + C_2$, $\varphi(K_2) = \tilde{\varphi}(C_2) = C_1$.
13. $\sigma(g) = g + \varphi\big(K(g)\big)$, z. B.

$g = (1, 1, 0, 0, 0, 0, 1) = [(1, 0, 0, 0, 0, 0, 0) + B_1] + [(0, 0, 0, 0, 0, 1, 0) + B_5]$,
d. h., g liegt in der Klasse $K(g) = K_1 + K_2$. Nun ist

$$\varphi(K_1 + K_2) = \varphi(K_1) + \varphi(K_2) = (C_1 + C_2) + C_1 = C_2 = B_4 + B_5 = (0,0,0,0,1,1,1)$$

und damit

$$\sigma(g) = \sigma[(1, 1, 0, 0, 0, 0, 1)] = g + B_4 + B_5 = (1, 1, 0, 0, 1, 1, 0)$$
$$= a_1 + a_2 + a_5 + a_6.$$

14. $$\mathfrak{D}_{2,5} = \mathfrak{C}_2\mathfrak{B}_{2,5} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

$$\mathfrak{A}_7^* = \begin{pmatrix} \mathfrak{E}_5 & 0 \\ \mathfrak{D}_{2,5} & \mathfrak{E}_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

15. $$\mathfrak{M}_7 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Durch passende Zeilenumformungen nach Hilfssatz 1 und nach Hilfssatz 2 geht $\mathfrak{M}_7$ in

$$\mathfrak{M}_7^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

über. Schließlich erhält man aus $\mathfrak{M}_7^{-1}$, $\mathfrak{A}_7^*$ und $\mathfrak{M}_7$ die Matrix

$$\mathfrak{A}_7 = \mathfrak{M}_7^{-1}\mathfrak{A}_7^*\mathfrak{M}_7 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

In der Tat ist auch $\mathfrak{A}_7^2 \equiv \mathfrak{E}_7 \bmod 2$. (Alle Rechnungen wurden natürlich mod 2 durchgeführt.) Mit $\mathfrak{A}_7$ ergibt sich dann der folgende Automorphismus σ der Ordnung 2 von G:

$$\begin{aligned} \sigma(a_1) &= a_1 + a_4 + a_5 + a_6, \\ \sigma(a_2) &= a_2 + a_4 + a_7, \\ \sigma(a_3) &= a_3 + a_4 + a_7, \\ \sigma(a_4) &= a_4, \\ \sigma(a_5) &= a_4 + a_5 + a_7, \\ \sigma(a_6) &= a_4 + a_6 + a_7, \\ \sigma(a_7) &= a_7. \end{aligned}$$

§ 8. Bestimmung der Anzahl aller Automorphismen der Ordnung 2 von G im Fall $p \neq 2$

Grundlage für die Bestimmung der Anzahl $\mathrm{Aut}_2(G, p)$ aller Automorphismen der Ordnung 2 von G im Fall $p \neq 2$ liefert der Satz 4. Danach ist $\mathrm{Aut}_2(G, p)$ gleich der Anzahl aller möglichen Darstellungen von G als direkter Summe $G = U + U'$ zweier Untergruppen U und U' von G unter Berücksichtigung der Reihenfolge der Summanden. Nach Satz 15 ist nun jede Untergruppe U von G ein direkter Summand von G. Ist der Rang n von G größer als 1 und U eine feste Untergruppe von G mit $o(U) = p^k$, $1 \leqq k \leqq n-1$, so gibt es nach Satz 17 zu U offenbar so viele verschiedene Untergruppen U' von G mit $G = U + U'$, wie es geordnete Auswahlen vom Umfang $n - k$ mit Wiederholungen von Elementen aus U gibt. Die Anzahl dieser Auswahlen werde mit $N_{n,k}$ bezeichnet. Nach ([1], S. 50) ist

$$N_{n,k} = p^{k(n-k)}. \tag{57}$$

Zu festem k mit $1 \leqq k \leqq n-1$ werde durch $U_{n,k}$ die Anzahl aller Untergruppen U von G mit $o(U) = p^k$ bezeichnet. Nach [3], S. 53, gilt für $U_{n,k}$ die Formel

$$U_{n,k} = \frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-k+1} - 1)}{(p - 1)(p^2 - 1) \cdots (p^k - 1)}. \tag{58}$$

Die Untergruppen U von G mit $o(U) = p^k$, $1 \leqq k \leqq n-1$, liefern also $U_{n,k} \cdot N_{n,k}$ Darstellungen von G in der Form $G = U \dotplus U'$ und damit $U_{n,k} \cdot N_{n,k}$ Automorphismen der Ordnung 2 von G. Da man für $k = 0$ nur die Darstellung $G = \{0\} \dotplus G$ und für $k = n$ nur die Darstellung $G = G \dotplus \{0\}$, d. h. nach Bemerkung 1 den Automorphismus τ bzw. den identischen Automorphismus ε erhält, ergibt sich für $\mathrm{Aut}_2(G, p)$ schließlich

$$\mathrm{Aut}_2(G, p) = 2 + \sum_{k=1}^{n-1} U_{n,k} \cdot N_{n,k}. \tag{59}$$

Im Fall $n = 1$ gibt es nur den identischen Automorphismus ε und den Automorphismus τ aus Bemerkung 1 als einzige Automorphismen der Ordnung 2 von G. Mithin ergibt sich unter Berücksichtigung von (57) und (58) als Resultat der folgende Satz.

Satz 19. *Ist G eine endliche elementare abelsche Gruppe vom Rang $n \geqq 1$ für die Primzahl $p \neq 2$, so gilt für die Anzahl $\mathrm{Aut}_2(G, p)$ der Automorphismen σ der Ordnung 2 von G (unter Einschluß des identischen Automorphismus $\sigma = \varepsilon$) die Formel*

$$\mathrm{Aut}_2(G, p) = \begin{cases} 2 & \text{für } n = 1, \\ 2 + \sum_{k=1}^{n-1} \dfrac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-k+1} - 1)}{(p - 1)(p^2 - 1) \cdots (p^k - 1)} p^{k(n-k)} & \text{für } n \geqq 2. \end{cases} \tag{60}$$

Bemerkung 6. Gemäß den Ausführungen in der Einleitung liefert die Formel (60) dann natürlich auch die Anzahl der Lösungen der Matrizenkongruenz $\mathfrak{X}_n^2 \equiv \mathfrak{E}_n \bmod p$ für $p \neq 2$.

Bemerkung 7. Der Ausdruck

$$\frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-k+1} - 1)}{(p - 1)(p^2 - 1) \cdots (p^k - 1)} p^{k(n-k)} \tag{61}$$

hat für $k = i$ und für $k = n - i$ denselben Wert, denn es ist offenbar

$$(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-i+1} - 1)(p^{n-i} - 1) \cdots (p^2 - 1)(p - 1)\, p^{i(n-i)}$$
$$= (p^n - 1)(p^{n-1} - 1) \cdots (p^{i+1} - 1)(p^i - 1) \cdots (p^2 - 1)(p - 1)\, p^{i(n-i)},$$

woraus durch Division sofort

$$\frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-i+1} - 1)}{(p - 1)(p^2 - 1) \cdots (p^i - 1)} p^{i(n-i)} = \frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{i+1} - 1)}{(p - 1)(p^2 - 1) \cdots (p^{n-i} - 1)} p^{(n-i)i}$$
$$= \frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-(n-i)+1} - 1)}{(p - 1)(p^2 - 1) \cdots (p^{n-i} - 1)} p^{(n-i)[n-(n-i)]}$$

folgt, was die Gleichheit von (61) für $k = i$ und für $k = n - i$ ergibt. In (60) braucht also in der rechts stehenden Summe nur bis $\dfrac{n-1}{2}$ bei ungeradem n bzw. bis $\dfrac{n}{2} - 1$

bei geradem n addiert und die entstehende Summe mit 2 multipliziert zu werden. Bei geradem n muß aber anschließend noch der Summand für $k = \frac{n}{2}$ hinzuaddiert werden. Um zu einer einheitlichen Schreibweise zu kommen, kann

$$N = \frac{n-1}{2} - \left(\frac{1}{4} + (-1)^n \frac{1}{4}\right) \tag{62a}$$

und

$$M = 1 - \left(\frac{1}{2} + (-1)^{n+1} \frac{1}{2}\right) \tag{62b}$$

gesetzt werden, womit sich dann (60) in der folgenden Form schreiben läßt:

$$\mathrm{Aut}_2(G, p) = \begin{cases} 2 & \text{für } n = 1, \\ 2 + 2\sum\limits_{k=1}^{N} \dfrac{(p^n-1)(p^{n-1}-1)\cdots(p^{n-k+1}-1)}{(p-1)(p^2-1)\cdots(p^k-1)}\, p^{k(n-k)} \\ \quad + M \dfrac{(p^n-1)(p^{n-1}-1)\cdots(p^{n-N}-1)}{(p-1)(p^2-1)\cdots(p^{N+1}-1)}\, p^{(N+1)(n-N-1)} & \text{für } n \geqq 2. \end{cases} \tag{62}$$

Beispiel. Im Fall $n = 4$, $p = 3$ ist

$$N = \frac{4-1}{2} - \left(\frac{1}{4} + (-1)^4 \frac{1}{4}\right) = 1, \quad M = 1 - \left(\frac{1}{2} + (-1)^5 \frac{1}{2}\right) = 1,$$

also

$$\mathrm{Aut}_2(G, p) = \mathrm{Aut}_2(G, 3) = 2 + 2 \cdot \frac{3^4 - 1}{3 - 1} \cdot 3^3 + 1 \cdot \frac{(3^4-1)(3^3-1)}{(3-1)(3^2-1)} \cdot 3^4$$
$$= 2 + 2 \cdot \frac{80}{2} \cdot 27 + \frac{80 \cdot 26}{2 \cdot 8} \cdot 81 = 2 + 80 \cdot 27 + 130 \cdot 81 = 12692,$$

d. h., eine (endliche) elementare abelsche Gruppe G vom Typus (3, 3, 3, 3) besitzt 12692 Automorphismen der Ordnung 2, bzw. die Matrizenkongruenz

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \bmod 3$$

hat 12692 Lösungen. Alle diese 12692 Automorphismen bzw. Lösungen lassen sich nach § 6 explizit angeben.

§ 9. Bestimmung der Anzahl aller Automorphismen der Ordnung 2 von G im Fall $p = 2$

Grundlage für die Bestimmung der Anzahl $\mathrm{Aut}_2(G, p)$ aller Automorphismen der Ordnung 2 von G im Fall $p = 2$ liefert der Satz 10. Danach ist $\mathrm{Aut}_2(G, p) = \mathrm{Aut}_2(G, 2)$ gleich der Anzahl der Tripel (U', U^*, φ), wobei U', U^* ein Untergruppen-

paar von G mit $\{0\} \subset U'$, $U^* \subseteq U'$, $o(U^*) \cdot o(U') = o(G)$ und φ ein Isomorphismus von G/U' auf U^* ist. Wenn der Rang n von G gleich 1 ist, existiert nur ein Tripel dieser Art, nämlich das Tripel $(G, \{0\}, \varphi)$, wobei φ der triviale Isomorphismus von G/G auf $\{0\}$ ist. Mithin ist in diesem Fall $\mathrm{Aut}_2(G, 2) = 1$. Ist $n \geqq 2$ und $U' = G$, so existiert zu U' auch nur ein einziges Tripel der obigen Art, nämlich ebenfalls das Tripel $(G, \{0\}, \varphi)$ mit φ wie vorhin. Die Untergruppe $U' = G$ von G liefert also nur einen einzigen Automorphismus von G, nämlich den identischen Automorphismus $\sigma = \varepsilon$ von G. Als weitere Untergruppen U' von G kommen dann nur diejenigen der Ordnung 2^r in Betracht mit

$$\frac{n}{2} + \left(\frac{1}{4} + (-1)^{n+1}\frac{1}{4}\right) = R \leqq \nu \leqq n - 1$$

(§ 5, Abschnitt 1). Zu jeder solchen Untergruppe U' existieren dann $U_{\nu,n-\nu}$ (Bezeichnung wie in § 8) Untergruppen U^* der Ordnung $2^{n-\nu}$ von U' mit $o(U^*) \cdot o(U') = o(G) = 2^n$. Nach § 5, Abschnitt 2, ist die Anzahl $A_{n-\nu}$ der Isomorphismen von G/U' auf U^* gleich der Anzahl der Automorphismen von U^*. Eine Untergruppe U' der Ordnung 2^r von G mit $R \leqq \nu \leqq n - 1$ liefert also $U_{\nu,n-\nu} \cdot A_{n-\nu}$ Automorphismen σ der Ordnung 2 von G. Da zu jedem ν mit $R \leqq \nu \leqq n - 1$ gerade $U_{n,\nu}$ Untergruppen U' der Ordnung 2^r von G existieren, ist also, wenn noch $U' = G$ mit berücksichtigt wird, im Fall $n \geqq 2$

$$\mathrm{Aut}_2(G, 2) = 1 + \sum_{\nu=R}^{n-1} U_{n,\nu} \cdot U_{\nu,n-\nu} \cdot A_{n-\nu}. \tag{63}$$

Nach [2], S. 116, ist

$$A_s = p^{s^2(\beta-1)} \prod_{\tau=1}^{s} (p^s - p^{\tau-1})$$

die Ordnung der Automorphismengruppe einer endlichen abelschen Gruppe der Ordnung p^s und vom Typus $(p^\beta, p^\beta, \ldots, p^\beta, s\text{-mal})$, wobei p eine beliebige Primzahl und $\beta \geqq 1$ ist. Im vorliegenden Fall ist also

$$A_{n-\nu} = (2^{n-\nu} - 1)(2^{n-\nu} - 2)(2^{n-\nu} - 2^2) \cdots (2^{n-\nu} - 2^{n-\nu-1})$$

(siehe auch [4], S. 106) oder

$$\begin{aligned} A_{n-\nu} &= 2 \cdot 2^2 \cdots 2^{n-\nu-1}(2^{n-\nu} - 1)(2^{n-\nu-1} - 1)(2^{n-\nu-2} - 1) \cdots (2^1 - 1) \\ &= 2^{\frac{(n-\nu)(n-\nu-1)}{2}} (2^{n-\nu} - 1)(2^{n-\nu-1} - 1)(2^{n-\nu-2} - 1) \cdots (2^1 - 1). \end{aligned}$$

Entsprechend (58) gilt ferner

$$U_{n,\nu} = \frac{(2^n - 1)(2^{n-1} - 1) \cdots (2^{n-\nu+1} - 1)}{(2^1 - 1)(2^2 - 1) \cdots (2^\nu - 1)}$$

und

$$U_{\nu,n-\nu} = \frac{(2^\nu - 1)(2^{\nu-1} - 1) \cdots (2^{2\nu-n+1} - 1)}{(2^1 - 1)(2^2 - 1) \cdots (2^{n-\nu} - 1)}.$$

Mithin gilt der folgende Satz.

Satz 20. *Ist G eine endliche elementare abelsche Gruppe vom Rang $n \geqq 1$ für die Primzahl $p = 2$, so gilt für die Anzahl* $\mathrm{Aut}_2(G, p) = \mathrm{Aut}_2(G, 2)$ *der Automorphismen σ*

der Ordnung 2 von G (unter Einschluß des identischen Automorphismus $\sigma = \varepsilon$)

$$\mathrm{Aut}_2(G,2) = \begin{cases} 1 & \text{für } n = 1, \\ 1 + \sum_{\nu=R}^{n-1} 2^{\frac{(n-\nu)(n-\nu-1)}{2}} (2^n-1)(2^{n-1}-1)\cdots(2^{n-\nu+1}-1) & \\ \quad \times \dfrac{(2^\nu-1)(2^{\nu-1}-1)\cdots(2^{2\nu-n+1}-1)}{(2^\nu-1)(2^{\nu-1}-1)\cdots(2^2-1)(2^1-1)} & \text{für } n \geqq 2, \\ \quad R = \dfrac{n}{2} + \left(\dfrac{1}{4} + (-1)^{n+1}\dfrac{1}{4}\right). & \end{cases} \tag{64}$$

Bemerkung 8. Wie im Fall $p \neq 2$ die Formel (60) so läßt sich auch hier im Fall $p = 2$ die Formel (64) für die Rechnung noch etwas vereinfachen. Offenbar ist für $\nu = R, R+1, \ldots, n-1$

$$\begin{aligned} K_\nu &= 2^{\frac{(n-\nu)(n-\nu-1)}{2}} (2^n-1)(2^{n-1}-1)\cdots(2^{n-\nu+1}-1) \cdot \\ &\quad \times \frac{(2^\nu-1)(2^{\nu-1}-1)\cdots(2^{2\nu-n+1}-1)}{(2^\nu-1)(2^{\nu-1}-1)\cdots(2^2-1)(2^1-1)} \\ &= 2^{\frac{(n-\nu)(n-\nu-1)}{2}} \frac{(2^n-1)(2^{n-1}-1)\cdots(2^{n-\nu+1}-1)}{(2^{2\nu-n}-1)(2^{2\nu-n-1}-1)\cdots(2^2-1)(2^1-1)} = B_\nu, \end{aligned} \tag{65}$$

allerdings unter der Voraussetzung $\nu > \dfrac{n}{2}$, was bei ungeradem n stets erfüllt ist. Weiterhin ist sicherlich

$$\begin{aligned} B_\nu &= 2^{\frac{(n-\nu)(n-\nu-n)}{2}} \frac{(2^n-1)(2^{n-1}-1)\cdots(2^{n-\nu+1}-1)}{(2^{2\nu-n}-1)(2^{2\nu-n-1}-1)\cdots(2^2-1)(2^1-1)} \\ &= 2^{\frac{(n-\nu)(n-\nu-1)}{2}} \frac{(2^n-1)(2^{n-1}-1)\cdots(2^{2\nu-n+1}-1)}{(2^{n-\nu}-1)(2^{n-\nu-1})\cdots(2^2-1)(2^1-1)} = C_\nu, \end{aligned} \tag{66}$$

falls $2\nu - n \geqq n - \nu + 1$, d. h. $3\nu \geqq 2n+1$, also $\nu \geqq \dfrac{2n+1}{3} = S^*$ ist. Nun ist bei ungeradem n offenbar $n - R + 1 = R$ und bei geradem n dagegen $n - R + 1 = R + 1$. Wird also von $\nu = n - R + 1$ an summiert, so ist stets $\nu > \dfrac{n}{2}$, und man kann, falls noch $n > 2$ ist,

$$\sum_{\nu=R}^{n-1} K_\nu = \sum_{\nu=n-R+1}^{n-1} B_\nu + MK_R \tag{67}$$

schreiben, wenn wieder $M = 1 - \left(\dfrac{1}{2} + (-1)^{n+1}\dfrac{1}{2}\right)$ gesetzt wird. M ist nur bei geradem n ungleich Null. Für gerades n ergibt sich durch Einsetzen in K_ν:

$$K_R = 2^{\frac{n}{8}(n-2)} (2^n-1)(2^{n-1}-1)\cdots(2^{n-R+1}-1). \tag{68}$$

Ist $n = 2$, so tritt die Summe $\sum_{\nu=n-R+1}^{n-1} B_\nu$ in (67) nicht auf, und man erhält aus (67)

$$\sum_{\nu=R}^{n-1} K_\nu = K_R. \tag{69}$$

Wird im Fall $n > 2$ die Summe $\sum_{\nu=n-R+1}^{n-1} B_\nu$ in (67) auf die Form

$$\sum_{\nu=n-R+1}^{n-1} B_\nu = \sum_{\nu=n-R+1}^{\nu<S^*} B_\nu + \sum_{\nu\geqq S^*}^{n-1} C_\nu \tag{70}$$

gebracht, wobei wie oben $S^* = \frac{2n+1}{3}$ ist, so tritt die zweite Summe rechts in (70) natürlich nur dann auf, wenn $n - 1 \geqq \frac{2n+1}{3}$, also $n \geqq 4$ ist. Damit die erste Summe rechts in (70) auftreten kann, muß $n - R + 1 < \frac{2n+1}{3}$, d. h. $n < 3R - 2$ gelten. Für gerades n, also für $R = \frac{n}{2}$, folgt dann $n < \frac{3}{2} n - 2$, d. h. $n > 4$, und für ungerades n, also für $R = \frac{n+1}{2}$, ist $n < \frac{3}{2}(n+1) - 2$, d. h. $n > 1$. Zusammenfassend läßt sich also die Formel (64) auch wie folgt schreiben:

$$\mathrm{Aut}_2(G, 2) = \begin{cases} 1 & \text{für } n = 1, \\ 1 + K_R & \text{für } n = 2, \\ 1 + \sum_{\nu=n-R+1}^{n-1} B_\nu & \text{für } n = 3, \\ 1 + \sum_{\nu=n-R+1}^{n-1} C_\nu + K_R & \text{für } n = 4, \\ 1 + \sum_{\nu=n-R+1}^{S} B_\nu + \sum_{\nu=S+1}^{n-1} C_\nu + MK_R & \text{für } n \geqq 5. \end{cases} \tag{71}$$

Hierbei ist

$$K_R = 2^{\frac{n}{8}(n-2)}(2^n - 1)(2^{n-1} - 1)\cdots(2^{n-R+1} - 1), \tag{71a}$$

$$B_\nu = 2^{\frac{(n-\nu)(n-\nu-1)}{2}} \frac{(2^n - 1)(2^{n-1} - 1)\cdots(2^{n-\nu+1} - 1)}{(2^{2\nu-n} - 1)(2^{2\nu-n-1} - 1)\cdots(2^2 - 1)(2^1 - 1)}, \tag{71b}$$

$$C_\nu = 2^{\frac{(n-\nu)(n-\nu-1)}{2}} \frac{(2^n - 1)(2^{n-1} - 1)\cdots(2^{2\nu-n+1} - 1)}{(2^{n-\nu} - 1)(2^{n-\nu-1} - 1)\cdots(2^2 - 1)(2^1 - 1)}. \tag{71c}$$

$$R = \frac{n}{2} + \left(\frac{1}{4} + (-1)^{n+1}\frac{1}{4}\right), \tag{71d}$$

$$M = 1 - \left(\frac{1}{2} + (-1)^{n+1}\frac{1}{2}\right), \tag{71e}$$

S = Größte positive ganze Zahl, die echt in $S^* = \frac{2n+1}{3}$ enthalten ist. (71f)

Bemerkung 9. Die Formel (71) hat gegenüber der Formel (64) den Vorteil, daß alle Faktoren der Form $2^j - 1$, die in (64) im Zähler und im Nenner gleichzeitig auftreten, in (71) weggekürzt sind.

Beispiel. Im Fall $n = 7$ ist $S = 4$, $R = 4$, $M = 0$, $n - R + 1 = 4$, also

$$\begin{aligned}\mathrm{Aut}_2(G, 2) &= 1 + B_4 + C_5 + C_6 \\ &= 1 + 2^{\frac{(7-4)(7-4-1)}{2}} \frac{(2^7-1)(2^6-1)(2^5-1)(2^4-1)}{(2^1-1)} \\ &\quad + 2^{\frac{(7-5)(7-5-1)}{2}} \frac{(2^7-1)(2^6-1)(2^5-1)(2^4-1)}{(2^2-1)(2^1-1)} \\ &\quad + 2^{\frac{(7-6)(7-6-1)}{2}} \frac{(2^7-1)(2^6-1)}{(2^1-1)} \\ &= 1 + 2^8 \cdot 127 \cdot 63 \cdot 31 \cdot 15 + 2^1 \cdot \frac{127 \cdot 63 \cdot 31 \cdot 15}{3} + 2^0 \cdot 127 \cdot 63 \\ &= 1 + 29763720 + 2480310 + 8001 = 32252032,\end{aligned}$$

d. h., eine (endliche) elementare abelsche Gruppe G vom Typus (2, 2, 2, 2, 2, 2, 2) besitzt 32252032 Automorphismen der Ordnung 2, bzw. die Matrizenkongruenz

$$\begin{pmatrix} x_{11} \dots x_{17} \\ \vdots \quad\quad \vdots \\ x_{71} \dots x_{77} \end{pmatrix} \equiv \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} \bmod 2$$

hat 32252032 Lösungen. Alle diese 32252032 Automorphismen bzw. Lösungen lassen sich nach § 7 explizit angeben.

LITERATUR

[1] FLACHSMEYER, J.: Kombinatorik. 3. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1972.

[2] LATT, K.: Zur Konstruktion der Automorphismen einer endlichen abelschen Gruppe. Math. Nachr. *45* (1970), 101–142.

[3] SPEISER, A.: Die Theorie der Gruppen von endlicher Ordnung. 4. Aufl., Birkhäuser-Verlag, Basel–Stuttgart 1956.

[4] ZASSENHAUS, H.: Lehrbuch der Gruppentheorie. B. G. Teubner, Leipzig–Berlin 1937 (engl. Ausgabe: The Theory of Groups, 2nd ed., Vandenhoeck & Ruprecht, Göttingen/ Chelsea, Publ. Comp., New York 1958 (Nachdrucke 1965 und 1967).

Manuskripteingang: 20. 2. 1978

VERFASSER:

KLAUS LATT, Sektion Mathematik der Humboldt-Universität Berlin