ACTA ARITHMETICA
XX (1972)

Über Permutationsfunktionen in mehreren Unbestimmten

von

RUDOLF LIDL (Wien)

Sei R ein kommutativer Ring mit Einselement. Man sagt, die Permutation π der Elemente von R wird dargestellt durch die rationale Funktion $h(x) = f(x)/g(x)$ (unter rationaler Funktion verstehen wir immer ein Element des Quotientenringes von $R[x]$), wenn $g(a)$ für jedes $a \in R$ eine Einheit von R ist und wenn gilt: $\pi(a) = h(a)$ für jedes $a \in R$. $h(x)$ heißt Permutationsfunktion von R, wenn es eine Permutation der Elemente von R darstellt. Permutationsfunktionen von kommutativen Ringen bzw. endlichen Körpern wurden in der Literatur schon öfter studiert (vgl. etwa L. Carlitz [1], W. Nöbauer [4], L. Redei [7]). Die Grundprobleme des ganzen Fragenkreises sind: Welche Permutationen von R lassen sich durch rationale Funktionen darstellen und welche rationalen Funktionen $h(x)$ über R sind Permutationsfunktionen? Zur Beantwortung der ersten Frage kann man folgendes sagen: Für endliche Ringe stimmt bekanntlich die Menge der durch rationale Funktionen darstellbaren Permutationen überein mit der Menge der durch Polynome darstellbaren Permutationen. Nach L. Redei und T. Szele [8] gilt: Genau dann lassen sich alle Permutationen von R durch Polynome darstellen, wenn R ein Galoisfeld ist. Das zweite Grundproblem wurde teilweise von W. Nöbauer in [4] behandelt und zwar gilt: Die rationale Funktion $h(x)$ über den ganzen Zahlen ist dann und nur dann Permutationsfunktion des Restklassenringes mod ab, $(a, b) = 1$, wenn sie Permutationsfunktion der Restklassenringe mod a und mod b ist. Sie ist genau dann Permutationsfunktion des Restklassenringes mod p^e, p Primzahl und $e > 1$, wenn sie Permutationsfunktion des Restklassenringes mod p ist und wenn gilt: $h'(a) \not\equiv 0 \bmod p$ für alle a.

Eine unmittelbare Übertragung der Definition der Permutationsfunktion auf den Fall von mehreren Unbestimmten ist nicht möglich, denn die durch die rationale Funktion $h(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n)$ dargestellte Abbildung ist eine Abbildung des n-fachen Cartesischen Produktes R^n in R, ist also für $n > 1$ keine Abbildung einer Menge in sich selbst und daher keine Permutation. Wir müssen also

n-Tupel von rationalen Funktionen betrachten, die Abbildungen von R^n in sich selbst darstellen. Wir geben nun die allgemeine Definition der Permutationsfunktion. Unter einer Funktion wollen wir im folgenden immer eine rationale Funktion, also ein Element des vollen Quotientenringes von $R[x_1, \ldots, x_n]$ verstehen. Sei I ein Ideal von R. Eine Funktion $h(x_1, \ldots, x_n)$ bezeichnen wir als *volldefiniert* mod I, wenn es eine Quotientendarstellung $h(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n)$ gibt, für die $g(a_1, \ldots, a_n) \bmod I$ für beliebige $(a_1, \ldots, a_n) \in R^n$ eine Einheit von R/I ist. Ist $h(x_1, \ldots, x_n)$ volldefiniert mod I, dann wird durch

$$(a_1 \bmod I, \ldots, a_n \bmod I) \to \frac{f(a_1, \ldots, a_n) \bmod I}{g(a_1, \ldots, a_n) \bmod I}$$

eine eindeutige Abbildung von $(R/I)^n$ in R/I definiert, die von der Wahl der Quotientendarstellung von $h(x_1, \ldots, x_n)$ unabhängig ist. Ein geordnetes n-Tupel $\mathfrak{h} = (h_1, \ldots, h_n)$ von Funktionen bezeichnen wir als *Funktionsvektor*.

Definition. Die Funktion $h(x_1, \ldots, x_n)$ heißt *Permutationsfunktion* mod I, wenn sie volldefiniert mod I ist und es einen Funktionsvektor $\mathfrak{h}$ aus volldefinierten Funktionen mod I mit $h(x_1, \ldots, x_n)$ als Komponente gibt, so daß die durch $\mathfrak{h}$ induzierte Abbildung von $(R/I)^n$ in sich eine Permutation ist.

Definition. Einen Funktionsvektor $\mathfrak{h}$, der aus volldefinierten Funktionen mod I besteht und eine Permutation von $(R/I)^n$ induziert, nennen wir *Permutationsfunktionsvektor* mod I.

Offensichtlich ist ein Funktionsvektor nur dann Permutationsfunktionsvektor mod I, wenn jede seiner Komponenten eine Permutationsfuntion mod I ist. Man sieht unmittelbar ein, daß die in [2] und [5] untersuchten Permutationspolynome mod I nur ein Spezialfall der Permutationsfunktionen mod I sind, denn es gilt: Ist $f(x_1, \ldots, x_n)$ ein Permutationspolynom mod I, dann ist die durch den Quotienten $f(x_1, \ldots, x_n)/e$ dargestellte rationale Funktion eine Permutationsfunktion mod I (wobei e das Einselement von R ist). Die beiden Grundprobleme der Theorie der Darstellung von Permutationen durch rationale Funktionen in einer Unbestimmten kann man auf Polynomfunktionen in mehreren Unbestimmten folgendermaßen übertragen: Welche Permutationen lassen sich durch Funktionsvektoren darstellen und welche Funktionsvektoren sind Permutationsfunktionsvektoren? Zum ersten Problem zeigte W. Nöbauer [6]: Bei beliebigem $n \geqslant 1$ lassen sich alle eindeutigen Abbildungen von R^n in sich genau dann rational darstellen, wenn R ein Galoisfeld ist. Die eindeutige Abbildung α von R^n in sich läßt sich rational darstellen soll heißen, daß es Polynome $f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)$ und einheitswertige Polynome $g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)$ in $R[x_1, \ldots, x_n]$ gibt

(ein Polynom heißt einheitswertig, wenn $g(a_1, \ldots, a_n)$ für alle $(a_1, \ldots, a_n) \in R^n$ eine Einheit von R ist), sodaß

$$\alpha(a_1, \ldots, a_n) = \left(\frac{f_1(a_1, \ldots, a_n)}{g_1(a_1, \ldots, a_n)}, \ldots, \frac{f_n(a_1, \ldots, a_n)}{g_n(a_1, \ldots, a_n)}\right)$$

für alle $(a_1, \ldots, a_n) \in R^n$.

Die Menge aller jener Permutationen von R^n, die sich durch rationale Funktionen darstellen lassen, bildet eine Unterhalbgruppe der symmetrischen Permutationsgruppe S_{R^n} des Rings R^n, falls R ein endlicher Ring ist also sogar eine Untergruppe von S_{R^n}.

Das zweite Grundproblem läßt sich — wie wir nun zeigen werden für die für uns interessanten Ringe mittels der beiden folgenden Sätze zurückführen auf Untersuchungen in endlichen Körpern. An Stelle des beliebigen Rings R in der allgemeinen Definition nehmen wir nun den Integritätsbereich Z der ganzen rationalen Zahlen, dann ist $I = (m)$, m natürliche Zahl, und es gilt die

Definition. Der Quotient $f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n)$ von ganzzahligen, teilerfremden Polynomen heißt *Permutationsfunktion* mod m, wenn er volldefiniert mod m ist und wenn es einen Funktionsvektor $\mathfrak{h}(x_1, \ldots, x_n)$ aus volldefinierten Funktionen mod m mit $f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n)$ als Komponente gibt, so daß $\mathfrak{h}$ eine Permutationsabbildung von $(Z/(m))^n$ auf sich induziert; d.h. wenn es einen Funktionsvektor $\mathfrak{h}(x_1, \ldots, x_n) = (f_1/g_1, \ldots, f_n/g_n)$ gibt, für den $g_i(a_1, \ldots, a_n)$ eine prime Restklasse mod m für jedes ganzzahlige n-Tupel $(a_1, \ldots, a_n)$ repräsentiert, für welchen die durch $\alpha(a_1, \ldots, a_n) \equiv \mathfrak{h}(a_1, \ldots, a_n) \bmod m$ definierte Abbildung eine Permutation von $(Z/(m))^n$ ist.

Satz 1. *Der Funktionsvektor $\mathfrak{h}$ ist genau dann ein Permutationsfunktionsvektor* mod m, $m = ab$, $(a, b) = 1$, *wenn er einer* mod a *und* mod b *ist.*

Beweis. Bekanntlich gilt: Sei $(a, b) = 1$ und $f(x_1, \ldots, x_n)$ ein ganzzahliges Polynom in n Unbestimmten und N bzw. N' die Zahl der inkongruenten Lösungen von $f(x_1, \ldots, x_n) \equiv 0 \bmod a$ bzw. mod b, dann ist die Anzahl der inkongruenten Lösungen der Kongruenz $f(x_1, \ldots, x_n) \equiv 0 \bmod ab$ gleich $N \cdot N'$. Sei nun $\mathfrak{h}$ ein Permutationsfunktionsvektor mod m, dann ist er auch einer mod a und mod b. Denn es ist $g_i(a_1, \ldots, a_n)$ stets zu a bzw. zu b prim. Da $\mathfrak{h}$ ein Permutationsfunktionsvektor mod m ist, ist für jedes System $k_1, \ldots, k_n$ das Kongruenzsystem $f_i(x_1, \ldots, x_n) \equiv k_i g_i(x_1, \ldots, x_n) \bmod m$ lösbar, daher auch mod a und mod b. Ist umgekehrt $\mathfrak{h}$ ein Permutationsfunktionsvektor mod a und mod b, dann ist $g_i(a_1, \ldots, a_n)$ stets zu a prim und zu b prim, daher auch zu $ab = m$. Weiters sind zu gegebenen $k_1, \ldots, k_n$ die Kongruenzen $f_i \equiv k_i g_i \bmod a$, $f_i \equiv k_i g_i \bmod b$ stets lösbar. Daher ist $\mathfrak{h}$ ein Permutationsfunktionsvektor mod m.

SATZ 2. *Der Funktionsvektor* $\mathfrak{h}$ *ist dann und nur dann ein Permutationsfunktionsvektor* mod p^e, (p *Primzahl*, $e > 1$ *natürliche Zahl*), *wenn er ein Permutationsfunktionsvektor* mod p *ist und für alle* $(r_1, \ldots, r_n) \in Z^n$ *als Argument gilt*:

$$D = \begin{vmatrix} \begin{vmatrix} g_1 & f_1 \\ \frac{\partial g_1}{\partial x_1} & \frac{\partial f_1}{\partial x_1} \end{vmatrix} & \ldots & \begin{vmatrix} g_1 & f_1 \\ \frac{\partial g_1}{\partial x_n} & \frac{\partial f_1}{\partial x_n} \end{vmatrix} \\ \ldots\ldots\ldots\ldots\ldots \\ \begin{vmatrix} g_n & f_n \\ \frac{\partial g_n}{\partial x_1} & \frac{\partial f_n}{\partial x_1} \end{vmatrix} & \ldots & \begin{vmatrix} g_n & f_n \\ \frac{\partial g_n}{\partial x_n} & \frac{\partial f_n}{\partial x_n} \end{vmatrix} \end{vmatrix} \not\equiv 0 \bmod p.$$

Beweis. Sei $\mathfrak{h}$ ein Permutationsfunktionsvektor mod p und stets $D \not\equiv 0 \bmod p$, dann ist zu zeigen, daß $\mathfrak{h}$ auch Permutationsfunktionsvektor mod p^e ist. Wir zeigen das mittels vollständiger Induktion nach e. Für $e = 1$ ist $\mathfrak{h}$ nach Voraussetzung Permutationsfunktionsvektor mod p. Angenommen es sei gezeigt, daß $\mathfrak{h}$ auch einer mod p^{e-1} ist. Nach Definition heißt das, daß die $g_i(x_1, \ldots, x_n)$ für jeden ganzzahligen Vektor $(a_1, \ldots, a_n)$ eine prime Restklasse mod p^{e-1} repräsentieren und daß gilt: die Kongruenz $\mathfrak{h}(x_1, \ldots, x_n) \equiv (k_1, \ldots, k_n) \bmod p^{e-1}$ hat für alle ganzzahligen Vektoren $(k_1, \ldots, k_n)$ genau eine Lösung $(r_1, \ldots, r_n)$. Damit gleichbedeutend ist: die $g_i(x_1, \ldots, x_n)$ repräsentieren für jeden ganzzahligen Vektor $(a_1, \ldots, a_n)$ eine prime Restklasse mod p^{e-1} und die Vektorkongruenz

$$(1) \qquad (f_1 - k_1 g_1, \ldots, f_n - k_n g_n) \equiv (0, \ldots, 0) \bmod p^{e-1}$$

hat für jedes $(k_1, \ldots, k_n)$ genau eine Lösung. Diese beiden Bedingungen sind also nach Induktionsannahme erfüllt. Es sei $(r_1, \ldots, r_n)$ die Lösung von (1). Alle Lösungen von

$$(2) \qquad (f_1 - k_1 g_1, \ldots, f_n - k_n g_n) \equiv (0, \ldots, 0) \bmod p^e$$

sind von der Gestalt

$$(3) \qquad (r_1 + s_1 p^{e-1}, \ldots, r_n + s_n p^{e-1}) = \mathfrak{k}.$$

Wir haben daher die Lösungsvektoren von (2) unter den Vektoren der Gestalt (3) zu suchen. Wenn man den Vektor (3) in (2) einsetzt, dann erhält man den Vektor

$$\big(f_1(\mathfrak{k}) - k_1 g_1(\mathfrak{k}), \ldots, f_n(\mathfrak{k}) - k_n g_n(\mathfrak{k})\big).$$

Wir entwickeln diesen Vektor nach der Formel von Taylor. Wegen $2(e-1) \geqslant e$, $3(e-1) \geqslant e$, ... erhalten wir für $i = 1, 2, \ldots, n$

$$f_i(\mathfrak{k}) \equiv f_i(r_1, \ldots, r_n) + \sum_{v=1}^{n} s_v p^{e-1} \frac{\partial f_i(r_1, \ldots, r_n)}{\partial x_v} \bmod p^e,$$

$$g_i(\mathfrak{k}) \equiv g_i(r_1, \ldots, r_n) + \sum_{v=1}^{n} s_v p^{e-1} \frac{\partial g_i(r_1, \ldots, r_n)}{\partial x_v} \bmod p^e.$$

Daher ist der Vektor (3) dann und nur dann eine Lösung von (2), wenn folgendes Kongruenzensystem erfüllt ist:

$$f_1(r_1, \ldots, r_n) + p^{e-1} \sum_{v=1}^{n} s_v \frac{\partial f_1}{\partial x_v} - k_1 g_1(r_1, \ldots, r_n) - p^{e-1} k_1 \sum_{v=1}^{n} s_v \frac{\partial g_1}{\partial x_v} \equiv 0 \bmod p^e,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$f_n(r_1, \ldots, r_n) + p^{e-1} \sum_{v=1}^{n} s_v \frac{\partial f_n}{\partial x_v} - k_n g_n(r_1, \ldots, r_n) - p^{e-1} k_n \sum_{v=1}^{n} s_v \frac{\partial g_n}{\partial x_v} \equiv 0 \bmod p^e.$$

Wegen (1) ist dies genau dann erfüllt, wenn

$$(4) \qquad \begin{aligned} &\sum_{v=1}^{n} s_v \left(\frac{\partial f_1}{\partial x_v} - k_1 \frac{\partial g_1}{\partial x_v} \right) \equiv \frac{k_1 g_1 - f_1}{p^{e-1}} \bmod p, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\sum_{v=1}^{n} s_v \left(\frac{\partial f_n}{\partial x_v} - k_n \frac{\partial g_n}{\partial x_v} \right) \equiv \frac{k_n g_n - f_n}{p^{e-1}} \bmod p. \end{aligned}$$

Nun ist aber doch $(r_1, \ldots, r_n)$ Lösung von (1). Daraus folgt:

$$(5) \qquad k_i \equiv \frac{f_i(r_1, \ldots, r_n)}{g_i(r_1, \ldots, r_n)} \bmod p.$$

Daraus folgt:

$$\frac{\partial f_i}{\partial x_v} - k_i \frac{\partial g_i}{\partial x_v} \equiv g_i^{-1} \left(g_i \frac{\partial f_i}{\partial x_v} - f_i \frac{\partial g_i}{\partial x_v} \right) \bmod p$$

wobei als Argument $(r_1, \ldots, r_n)$ zu setzen ist. Daher ist (4) genau dann erfüllt, wenn das folgende System in den Unbekannten $s_1, \ldots, s_n$ erfüllt ist:

$$(6) \qquad \sum_{v=1}^{n} s_v \left(g_i \frac{\partial f_i}{\partial x_v} - f_i \frac{\partial g_i}{\partial x_v} \right) \equiv \frac{k_i g_i - f_i}{p^{e-1}} g_i \bmod p$$

für das Argument $(r_1, \ldots r_n)$ und $i = 1, 2, \ldots, n$.

Die Determinante dieses Gleichungssystems in $s_1, \ldots, s_n$ ist D. Nach Voraussetzung ist $D \not\equiv 0 \bmod p$, also hat das System (6) eine eindeutige Lösung $(s_1, \ldots, s_n) \bmod p$. Daraus folgt, daß das System (2) eine eindeutige Lösung k hat. Also ist der Satz in der einen Richtung gezeigt.

Sei nun umgekehrt $\mathfrak{h}$ ein Permutationsfunktionsvektor $\bmod p^e$. Dann ist $\mathfrak{h}$ auch einer $\bmod p$. Angenommen es sei $D \equiv 0 \bmod p$ für das Argument $(r_1, \ldots, r_n)$. Man setzt $k_i \equiv f_i(r_1, \ldots, r_n)/g_i(r_1, \ldots, r_n) \bmod p^e$ ein in die Kongruenz

$$(7) \quad \big(f_1(r_1, \ldots, r_n) - k_1 g_1(r_1, \ldots, r_n), \ldots, f_n(r_1, \ldots, r_n) - k_n g_n(r_1, \ldots, r_n)\big) \equiv (0, \ldots, 0) \bmod p^e.$$

Nach Voraussetzung ist $\mathfrak{h}$ ein Permutationsfunktionsvektor $\bmod p^e$, also auch einer $\bmod p^{e-1}$, d.h. (7) hat sowohl $\bmod p^e$ als auch $\bmod p^{e-1}$ genau eine Lösung $(r_1, \ldots, r_n)$. Alle Lösungen von (7) $\bmod p^e$ bekommt man durch das Verfahren im Hinreichend-Beweis. Dort kommt man auf das System (6). Die Determinante dieses Systems ist aber jetzt $\equiv 0 \bmod p$. Daraus folgt: Es gibt $\bmod p$ mehr als eine oder überhaupt keine Lösung $(s_1, \ldots, s_n)$. Daher ist (7) nicht eindeutig lösbar, im Widerspruch zur Voraussetzung. Also gilt $D \not\equiv 0 \bmod p$ und Satz 2 ist vollständig bewiesen.

Literatur

[1] L. Carlitz, *A note on permutation functions over a finite field*, Duke Math. Journ. 29 (1962), S. 325–332.

[2] R. Lidl, *Über Permutationspolynome in mehreren Unbestimmten*, Monatsh. Math. 75(1971), S. 432–440.

[3] W. Nöbauer, *Gruppen von Restklassen nach Restpolynomidealen*, Monatsh. Math. 59 (1955), S. 118–145.

[4] — *Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen*, Monatsh. Math. 69 (1965), S. 230–238.

[5] — *Zur Theorie der Polynomtransformationen und Permutationspolynome*, Math. Ann. 157 (1964), S. 332–342.

[6] — *Bemerkungen über die Darstellung von Abbildungen durch Polynome und rationale Funktionen*, Monatsh. Math. 68 (1964), S. 138–142.

[7] L. Redei, *Über eindeutig umkehrbare Polynome in endlichen Körpern*, Acta Scientiarium Math. 11 (1946–48), S. 85–92.

[8] — und T. Szele, *Algebraisch-zahlentheoretische Betrachtungen über Ringe I*, Acta Math. 79 (1947), S. 291–320.

IV. INSTITUT FÜR MATHEMATIK
Technische Hochschule, Wien

Eingegangen 18. 12. 1970 (128)

ACTA ARITHMETICA
XX (1972)

An application of Zassenhaus' unit theorem

by

HAROLD BROWN (Ohio)

In this note we present a direct application of Zassenhaus' generalized Dirichlet unit theorem [2] to the proof of an interesting result on orders with finite unit groups. This result is useful, e.g., in the determination of normalizers of finite unimodular groups [1].

THEOREM. *Let D be a finite dimensional division algebra over $\boldsymbol{Q}$, and let $\mathcal{O}$ be a maximal $\boldsymbol{Z}$-order in D. Then $U(\mathcal{O})$, the unit group of $\mathcal{O}$, is finite if and only if D is $\boldsymbol{Q}$-isomorphic to $\boldsymbol{Q}$, an imaginary quadratic extension of $\boldsymbol{Q}$, or a positive definite quaternion algebra over $\boldsymbol{Q}$.*

Proof. Let $\boldsymbol{R}\mathcal{O}$ denote the tensor product of $\boldsymbol{R}$ and $\mathcal{O}$. Since $\mathcal{O}$ contains a free $\boldsymbol{Q}$-basis for D, $\boldsymbol{R}\mathcal{O} \cong \boldsymbol{R} \otimes_{\boldsymbol{Q}} D$. We will show that if $U(\mathcal{O})$ is finite, then $\boldsymbol{R}\mathcal{O}$ is a division algebra over $\boldsymbol{R}$.

Let $\varphi\colon \boldsymbol{R}\mathcal{O} \to \mathrm{Hom}(\boldsymbol{R}\mathcal{O}, \boldsymbol{R}\mathcal{O})$ be the left regular representation of $\boldsymbol{R}\mathcal{O}$, and for any $x \in \boldsymbol{R}\mathcal{O}$ and any $\boldsymbol{R}$-basis B for $\boldsymbol{R}\mathcal{O}$, let $\hat{\varphi}_B(x)$ be the matrix of $\varphi(x)$ with respect to B. For $x \in \boldsymbol{R}\mathcal{O}$, let $\|x\|$ denote the regular norm of x, i.e. $\|x\| = \det \hat{\varphi}_B(x)$.

Consider $L(\mathcal{O}) = \{x \in \boldsymbol{R}\mathcal{O} \mid \|x\| = \pm 1\}$. $L(\mathcal{O})$ is clearly closed under multiplication, and for any $x \in L(\mathcal{O})$, $\|x\| = \det \hat{\varphi}_B(x) \neq 0$ implies x is not a left zero divisor in $\boldsymbol{R}\mathcal{O}$. Since $\boldsymbol{R}\mathcal{O}$ is finite dimensional over $\boldsymbol{R}$, there exists $y \in \boldsymbol{R}\mathcal{O}$ such that $xy = 1$. Therefore, $\hat{\varphi}_B(y) = \hat{\varphi}_B(x)^{-1}$ and $\hat{\varphi}_B(y)\hat{\varphi}_B(x) = I_n$. Since the regular representation is faithful, we have $yx = 1$, i.e. $y = x^{-1}$. Thus $L(\mathcal{O})$ is a subgroup of the unit group of $\boldsymbol{R}\mathcal{O}$. Also, $L(\mathcal{O})$ contains $U(\mathcal{O})$. For if we choose B as an integral basis for $\mathcal{O}$, then $x \in U(\mathcal{O})$ implies $\hat{\varphi}_B(x)$ and $\hat{\varphi}_B(x^{-1}) = \hat{\varphi}_B(x)^{-1}$ are integral matrices. Thus $\|x\| = \pm 1$.

Let $t = \dim_{\boldsymbol{R}} \boldsymbol{R}\mathcal{O} = \mathrm{rank}\, \mathcal{O}$, and let $L(\mathcal{O})$ have the topology induced by the usual Euclidean topology on $M_{t\times t}(\boldsymbol{R})$. $L(\mathcal{O})$ is a Lie group with respect to this topology(1). By Zassenhaus' theorem $U(\mathcal{O})$ is a discrete subspace of $L(\mathcal{O})$ with compact factor space. Thus, if $U(\mathcal{O})$ is finite, $L(\mathcal{O})$ must be compact, i.e. closed and bounded.

(1) Note that we could equivalently use the topology of $\boldsymbol{R}\mathcal{O}$ as a t-dimensional real manifold as $\hat{\varphi}_B$ is a topological isomorphism.