Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 15 (1942-1943)

Artikel: Gruppentheoretischer Beweis des Satzes von Hurwitz-Radon über die Komposition quadratischer Formen.

Autor: Eckmann, Beno

DOI: https://doi.org/10.5169/seals-14899

Gruppentheoretischer Beweis des Satzes von Hurwitz-Radon über die Komposition quadratischer Formen

Von Beno Eckmann, Lausanne

A. Hurwitz hat in der Arbeit „Über die Komposition der quadratischen Formen“ [1][1]) die Aufgabe behandelt, n Bilinearformen $z_1, \ldots, z_n$ der beiden Variabelnreihen $x_1, \ldots, x_p$ und $y_1, \ldots, y_n$ mit komplexen Koeffizienten so zu bestimmen, daß die Identität

$$(x_1^2 + \cdots + x_p^2)\,(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2$$

besteht. Er hat diejenigen ganzen Zahlen p und n bestimmt, für welche die Aufgabe lösbar ist, und in diesem Fall das Verfahren zur Konstruktion der allgemeinsten Lösungen explizite angegeben; man kann übrigens diese Lösungen immer reell wählen (vgl. Nr. 7). Dieselbe Aufgabe ist später mit einer andern Methode für reelle Koeffizienten von J. Radon [2] gelöst worden; in seiner Formulierung lautet das Resultat: *n sei von der Form $n = u \cdot 2^{4\alpha+\beta}$ (u ungerade, $\beta = 0, 1, 2, 3$); es gibt dann und nur dann (reelle) Bilinearformen mit der genannten Eigenschaft, wenn $p \leqslant 8\alpha + 2^\beta$ ist.* Als Spezialfall ist hierin der Satz enthalten, daß es solche Bilinearformen mit $p = n$ genau für $n = 1, 2, 4$ und 8 gibt; den Beweis hiefür hat Hurwitz schon in einer frühern Arbeit [3] erbracht.

In der vorliegenden Arbeit soll der Hurwitz-Radon'sche Satz mit Hilfe einiger grundlegender Sätze der *Darstellungstheorie* der endlichen Gruppen neu bewiesen werden. Unser Beweis ist sowohl vom Hurwitzschen als auch vom Radon'schen vollständig verschieden, lehnt sich aber im ersten Teil an den gruppentheoretischen Beweis an, welcher für den Spezialfall $p = n$ in einer Arbeit von Jordan, v. Neumann und Wigner [4] angegeben worden ist. Es erscheint aus folgenden Gründen nicht überflüssig, zu den Beweisen von Hurwitz und Radon noch einen dritten hinzuzufügen: einmal ist unser Beweis einfacher und kürzer — dafür operiert er aber mit weniger elementaren Begriffen und Sätzen; ferner sind die Methoden von Hurwitz wie auch von Radon ad hoc konstruiert und liegen außerhalb der sonst in der Algebra üblichen, während wir die Frage in die wohlbekannten Gedankengänge der Darstellungstheorie

[1]) Die Zahlen in eckiger Klammer [ ] verweisen auf das Literaturverzeichnis am Schluß der Arbeit.

einordnen, wo sie als schönes Beispiel für die Anwendung allgemeiner Sätze erscheint.

Wir lassen für die Koeffizienten der Bilinearformen *komplexe Zahlen* zu; es wird sich von selbst herausstellen, daß die Lösungen in reelle übergeführt werden können.

1. Wie Hurwitz und Radon ausführen[2]), ist die ursprüngliche Aufgabe mit dem folgenden *Matrizenproblem* äquivalent:

Es sind p komplexe orthogonale n-reihige Matrizen $A_1, \ldots, A_p$ zu bestimmen, welche die Relationen

$$A_k A_l' + A_l A_k' = 0\,, \qquad k\,, l = 1, \ldots, p\,;\ k \neq l \tag{1}$$

erfüllen. (B' bedeutet die Transponierte der Matrix B.) Der Fall $p = 1$ ist trivial, wir setzen $p \geqslant 2$ voraus.

Da man aus jeder Lösung dieser Aufgabe eine andere erhält, wenn man alle Matrizen $A_1, \ldots, A_p$ (etwa von links) mit einer beliebigen orthogonalen Matrix multipliziert, kann man annehmen, daß $A_p = E$ ist; dann ist $A_k' + A_k = 0$ für $k = 1, \ldots, p-1$, also

$$A_k A_l + A_l A_k = 0 \qquad k, l = 1, \ldots, p-1;\ k \neq l$$

und wegen $A_k A_k' = E$

$$A_k^2 = -E\,, \qquad k = 1, \ldots, p-1\,,$$

und diese beiden Relationen sind für $A_p = E$ mit (1) äquivalent.

Es genügt also, die Aufgabe in der Form zu behandeln:

Es sind $p-1$ komplexe orthogonale n-reihige Matrizen $A_1, \ldots, A_{p-1}$ zu bestimmen, welche die Relationen

$$A_k^2 = -E, A_k A_l = -A_l A_k\,, \qquad k, l = 1, \ldots, p-1; k \neq l \tag{2}$$

erfüllen.

2. Wir betrachten die abstrakte Gruppe G, die durch p Erzeugende $a_1, a_2, \ldots, a_{p-1}, \varepsilon$ und durch die Relationen

$$\varepsilon^2 = 1\,,\ a_k^2 = \varepsilon\,,\ \varepsilon a_k = a_k \varepsilon\,,\ a_k a_l = \varepsilon a_l a_k\,,\ (k, l = 1, \ldots, p-1\,;\ k \neq l)$$

gegeben ist. Man kann die Aufgabe, wie sie am Schluß von Nr. 1 formuliert ist, so aussprechen:

---

[2]) Vgl. [1], Abschnitt II, oder [2], Abschnitt II, 1.

Es ist eine Darstellung[3]) *der Gruppe G durch komplexe, n-reihige, orthogonale Matrizen gesucht, bei welcher ε durch die Matrix $-E$ dargestellt wird.*

Wir bestimmen zunächst, ohne uns um die Orthogonalität zu kümmern, die Grade der *irreduziblen* Darstellungen von G, suchen dann diejenigen Darstellungen, bei welchen ε durch $-E$ dargestellt wird und setzen sie zu solchen Darstellungen von gegebenem Grade n zusammen, die orthogonalen äquivalent sind.

3. Man erhält alle Elemente von G, wenn man in

$$a_{k_1} a_{k_2} \cdots a_{k_r} \quad \text{und} \quad \varepsilon a_{k_1} a_{k_2} \cdots a_{k_r} \ , \qquad r = 0, \ldots, p-1$$

die k_i alle Zahlen von $1, \ldots, p-1$ so durchlaufen läßt, daß

$$k_1 < k_2 < \cdots < k_r$$

ist. G hat also die Ordnung $2 \cdot 2^{p-1} = 2^p$; die Elemente sind, ausführlich geschrieben:

$$\begin{matrix} 1\,; \ a_1, \ldots, \ a_{p-1}\,; \ a_1 a_2, \ldots\,; \ \ldots\,; \ a_1 a_2 \ldots a_{p-1}\,; \\ \varepsilon\,; \ \varepsilon a_1, \ldots, \ \varepsilon a_{p-1}\,; \ \varepsilon a_1 a_2, \ldots\,; \ \ldots\,; \ \varepsilon a_1 a_2 \ldots a_{p-1}\,. \end{matrix} \tag{3}$$

Für $p = 2$ handelt es sich um die zyklische Gruppe der Ordnung 4, deren 4 irreduzible Darstellungen bekannt sind; wir setzen deshalb für das Folgende $p \geqslant 3$.

Die Kommutatoren von G sind offenbar alle $= 1$ oder $= \varepsilon$; die Kommutatorgruppe K hat die Ordnung 2 und die abelsch gemachte Gruppe $G' = G/K$ die Ordnung 2^{p-1}. *G besitzt also 2^{p-1} nicht-äquivalente Darstellungen vom Grade* 1.

4. Als Konjugiertes eines Elementes g von G kommt außer g höchstens εg in Frage. Genauer:

$$g = a_{k_1} a_{k_2} \cdots a_{k_r} \qquad (1 \leqslant r \leqslant p-2)$$

ist zu εg konjugiert, ebenso $g = a_1 a_2 \cdots a_{p-1}$ bei ungeradem p; 1, ε und, bei geradem p, $a_1 a_2 \cdots a_{p-1}$ und $\varepsilon a_1 a_2 \cdots a_{p-1}$ sind nur zu sich konjugiert (bilden das Zentrum von G).

[3]) Bezüglich aller im folgenden benützten Grundbegriffe und Sätze aus der Darstellungstheorie der endlichen Gruppen verweisen wir z. B. auf das 11. und 12. Kap. des Buches von *A. Speiser*, Theorie der Gruppen von endlicher Ordnung (2. Aufl., Berlin 1927).

Beweis:

a) $g = a_{k_1} a_{k_2} \dots a_{k_r}$, $1 \leqslant r \leqslant p-1$, r gerade.

$$a_{k_1}^{-1} g a_{k_1} = \varepsilon a_{k_1} a_{k_1} a_{k_2} \dots a_{k_r} a_{k_1} = a_{k_2} \dots a_{k_r} a_{k_1} = \varepsilon^{r-1} a_{k_1} a_{k_2} \dots a_{k_r},$$

also

$$a_{k_1}^{-1} g a_{k_1} = \varepsilon g .$$

b) $g = a_{k_1} a_{k_2} \dots a_{k_r}$, $1 \leqslant r \leqslant p-2$, r ungerade.

k sei eine der Zahlen $1, 2, \dots, p-1$, aber von $k_1, k_2, \dots, k_r$ verschieden.

$$a_k^{-1} g a_k = \varepsilon a_k a_{k_1} a_{k_2} \dots a_{k_r} a_k = \varepsilon\, \varepsilon^r a_k^2 a_{k_1} a_{k_2} \dots a_{k_r} = \varepsilon^{r+2} a_{k_1} a_{k_2} \dots a_{k_r},$$

also

$$a_k^{-1} g a_k = \varepsilon g .$$

c) $g = a_1 a_2 \cdots a_{p-1}$, p gerade.

Wir haben zu zeigen, daß für jedes Element b der Gruppe $b^{-1} g b = g$ ist. Es genügt, dies für die Erzeugenden $a_1, a_2, \dots, a_{p-1}$, ε zu beweisen. Für ε ist es trivial, für a_k $(k = 1, \dots, p-1)$ ist

$$a_k^{-1} g a_k = \varepsilon a_k a_1 a_2 \dots a_{p-1} a_k = \varepsilon\, \varepsilon^{p-2} a_k^2 a_1 a_2 \dots a_{p-1} = \varepsilon^p a_1 a_2 \dots a_{p-1},$$

also in der Tat

$$a_k^{-1} g a_k = g .$$

Die Anzahl h der Klassen konjugierter Elemente in G beträgt also:

$$h = 2^{p-1} + 2, \text{ wenn } p \text{ gerade,}$$

$$h = 2^{p-1} + 1, \text{ wenn } p \text{ ungerade ist.}$$

5. Da die Anzahl der nicht-äquivalenten irreduziblen Darstellungen $= h$ ist, gibt es außer den in Nr. 3 genannten Darstellungen ersten Grades bei ungeradem p noch eine irreduzible vom Grad $f > 1$, bei geradem p noch zwei von den Graden f und f', beide > 1. Da die Summe der Quadrate der Grade der irreduziblen Darstellungen gleich der Ordnung der Gruppe ist, hat man für die Grade f und f' die Gleichungen

a) wenn p ungerade ist:

$$f^2 + 2^{p-1} \cdot 1^2 = 2^p ,$$

also

$$f = 2^{\frac{p-1}{2}}$$

b) wenn p gerade ist:

$$f^2 + f'^2 + 2^{p-1} \cdot 1^2 = 2^p ,$$

also

$$f^2 + f'^2 = 2^{p-1} .$$

Da ferner f und f' Teiler der Gruppenordnung 2^p sind, etwa $f = 2^\nu$, $f' = 2^\mu$, so hat man

$$2^{2\nu} + 2^{2\mu} = 2^{p-1},$$

also

$$\nu = \mu = \frac{p-2}{2} ,$$

und

$$f = f' = 2^{\frac{p-2}{2}} .$$

6. Bei den 2^{p-1} Darstellungen vom Grade 1 wird ε durch $E = (+1)$ dargestellt. Bei den irreduziblen Darstellungen höhern Grades dagegen kann ε nicht durch die Einheitsmatrix dargestellt sein, da die Gruppe $G' = G/(1, \varepsilon)$ abelsch ist. Da ε im Zentrum liegt, muß die zugehörige Matrix, die mit allen Matrizen einer irreduziblen Darstellung vertauschbar ist, eine Diagonalmatrix λE sein, also wegen $\lambda^2 = 1$ die Matrix $-E$.

Es gibt also bei ungeradem p bis auf Äquivalenz *eine* irreduzible Darstellung, die für unsere Aufgabe verwendet werden kann, vom Grade $2^{\frac{p-1}{2}}$; bei geradem p gibt es deren *zwei*, vom Grade $2^{\frac{p-2}{2}}$ (gilt auch für $p = 2$). Für den Grad n einer beliebigen Darstellung von G, bei welcher ε in $-E$ übergeht, gilt somit

$$n = m \cdot 2^{\frac{p-1}{2}} , \text{ wenn } p \text{ ungerade,}$$

$$n = m \cdot 2^{\frac{p-2}{2}} , \text{ wenn } p \text{ gerade ist.}$$ [4])

(Dabei gibt es im ersten Fall bis auf Äquivalenz nur eine einzige, im zweiten dagegen $m + 1$ verschiedene Darstellungen.)

Eine Darstellung von G, bei welcher ε in $-E$ übergeht, vom Grade $n = u \cdot 2^t$ (u ungerade) ist also dann und nur dann möglich, wenn $p \leqslant 2t + 2$ ist. Mit andern Worten:

Es sei $n = u \cdot 2^t$ (u ungerade); es gibt dann und nur dann $p - 1$ komplexe n-reihige Matrizen $A_1, \ldots, A_{p-1}$, die den Gleichungen (2) *genügen, wenn $p \leqslant 2t + 2$* ist.[4])

[4]) Dieses Zwischenresultat findet sich auch bei *Hurwitz* [1], S. 657; wie dort ausgeführt wird, reicht es im Spezialfall $p = n$ schon zur vollständigen Diskussion aus.

$p \leqslant 2t + 2$ für $n = u \cdot 2^t$ ist also eine notwendige Bedingung für die Lösbarkeit der ursprünglichen Aufgabe.

7. Wir haben nun unter den gefundenen Darstellungen von G diejenigen zu suchen, welche *orthogonalen* Darstellungen äquivalent sind. Nach den Untersuchungen von Frobenius und Schur[5]) sind das dieselben, welche *reellen* Darstellungen (also orthogonalen *und* reellen) äquivalent sind. Jede Lösung der Darstellungsaufgabe oder der Hurwitz'schen Aufgabe ist also von selbst einer reellen Lösung äquivalent.

Eine Darstellung ist aber genau dann einer reellen äquivalent, wenn unter ihren irreduziblen Bestandteilen diejenigen, welche keinem reellen ähnlich sind, ebenso oft vorkommen wie ihre konjugiert-komplexen. Wir müssen also zunächst die irreduziblen Darstellungen von G, die für die Lösung unserer Aufgabe in Frage kommen, daraufhin untersuchen, ob sie reellen äquivalent sind oder nicht.

Zu diesem Zwecke bildet man[5]) die über die Gruppe G erstreckte Summe der Charaktere $\chi(g^2)$ der Quadrate der Elemente $g \in G$

$$S = \sum_{g \in G} \chi(g^2) \quad .$$

Eine irreduzible Darstellung D ist dann und nur dann einer reellen äquivalent, wenn die zugehörige Zahl $S > 0$ ist; wenn $S < 0$ ist, so ist D keiner reellen, aber der konjugiert-komplexen Darstellung $\overline{D}$ äquivalent, und wenn $S = 0$ ist, so sind auch D und $\overline{D}$ nicht äquivalent [5]).

Für ein beliebiges Element $g \in G$

$$g = a_{k_1} a_{k_2} \ldots a_{k_r} \quad \text{oder} \quad g = \varepsilon a_{k_1} a_{k_2} \ldots a_{k_r} \qquad \text{(vgl. (3))}$$

ist

$$g^2 = (a_{k_1} a_{k_2} \ldots a_{k_r})^2 = \varepsilon^{r+(r-1)+\cdots+2+1} = \varepsilon^{\frac{r(r+1)}{2}},$$

also

$$g^2 = 1, \text{ wenn } r \equiv 3{,}0 \pmod{4},$$
$$g^2 = \varepsilon, \text{ wenn } r \equiv 1{,}2 \pmod{4} \text{ ist.}$$

Geht bei der Darstellung D das Element ε in $-E$ über, und ist f ihr Grad, so ist also

$$\text{für } r \equiv 3{,}0 \pmod{4} \quad \chi(g^2) = f,$$
$$\text{für } r \equiv 1{,}2 \pmod{4} \quad \chi(g^2) = -f.$$

[5]) s. [5], bes. S. 186—187.

Summiert man über die 2^p Elemente von G, wie sie in (3) angegeben sind, so wird

$$S = 2f\,\sigma\,,$$

wo σ die von p allein abhängige Summe

$$\sigma = \binom{p-1}{0} - \binom{p-1}{1} - \binom{p-1}{2} + \binom{p-1}{3} + \binom{p-1}{4} - - \cdots \pm \binom{p-1}{p-1}$$

ist. Um das Vorzeichen von σ zu berechnen, betrachten wir die komplexe Zahl

$$z = (1 - i)^{p-1} = x + iy \quad (x, y \text{ reell})\ .$$

σ ist nichts anderes als $x + y$; das Vorzeichen von σ ist also in folgender Weise durch $\arg z = -\frac{\pi}{4}(p-1)$ bestimmt:

$$\sigma > 0\,,\ \text{wenn}\ -\frac{\pi}{4}(p-1) \equiv 0\,,\ \frac{\pi}{4}\,,\ \frac{2\pi}{4} \qquad (\text{mod. } 2\pi)\,,$$

$$\sigma = 0\,,\ \text{wenn}\ -\frac{\pi}{4}(p-1) \equiv \frac{3\pi}{4}\,,\ \frac{7\pi}{4} \qquad (\text{mod. } 2\pi)\,,$$

$$\sigma < 0\,,\ \text{wenn}\ -\frac{\pi}{4}(p-1) \equiv \frac{4\pi}{4}\,,\ \frac{5\pi}{4}\,,\ \frac{6\pi}{4}\,(\text{mod. } 2\pi)\ .$$

Die Summe S ist somit genau dann positiv, wenn $p \equiv 7, 0, 1$ (mod. 8) ist; für $p \equiv 3, 4, 5$ (mod. 8) ist S negativ, für $p \equiv 2, 6$ (mod. 8) ist $S = 0$.

Unsere irreduziblen Darstellungen von G sind also für $p \equiv 7, 0, 1$ (mod. 8) reellen Darstellungen äquivalent, für die übrigen p nicht; für $p \equiv 3, 4, 5$ sind sie den konjugiert-komplexen äquivalent, für $p \equiv 2$ und 6 nicht.

8. Der Grad n einer reellen Darstellung von G, bei welcher ε in $-E$ übergeht, muß somit für $p \not\equiv 7, 0, 1$ (mod. 8) ein gerades Vielfaches der Grade der irreduziblen Darstellungen sein. Der Grad einer reell-irreduziblen reellen Darstellung beträgt also

$$
\left.
\begin{array}{llll}
\text{a)}\ 2^{\frac{p-1}{2}} & \text{für} & p \equiv 7,1 & (\text{mod. } 8)\,, \\
\text{b)}\ 2^{\frac{p-2}{2}} & \text{für} & p \equiv 0 & (\text{mod. } 8)\,, \\
\text{c)}\ 2 \cdot 2^{\frac{p-1}{2}} = 2^{\frac{p+1}{2}} & \text{für} & p \equiv 3,5 & (\text{mod. } 8)\,, \\
\text{d)}\ 2 \cdot 2^{\frac{p-2}{2}} = 2^{\frac{p}{2}} & \text{für} & p \equiv 2,4,6 & (\text{mod. } 8)\,,
\end{array}
\right\} \qquad (4)
$$

und zwar gibt es für $p \equiv 0, 4$ (mod. 8) bis auf Äquivalenz zwei solche Darstellungen, für die übrigen p nur eine einzige.

Orthogonale Darstellungen der Gruppe G vom Grade $n = m \cdot 2^s$, bei welchen ε in $-E$ übergeht, gibt es also in folgenden Fällen:

$$
\begin{array}{llll}
\text{a)}\ s \equiv 3,0 & (\text{mod. } 4) & \text{und} & p = 2s + 1\,, \\
\text{b)}\ s \equiv 3 & (\text{mod. } 4) & \text{und} & p = 2s + 2\,, \\
\text{c)}\ s \equiv 2,3 & (\text{mod. } 4) & \text{und} & p = 2s - 1\,, \\
\text{d)}\ s \equiv 1,2,3 & (\text{mod. } 4) & \text{und} & p = 2s\,.
\end{array} \qquad (5)
$$
[6]

Bei gegebenem $n = u \cdot 2^t$ (u ungerade) beträgt also die *größtmögliche* Zahl p

$$
\begin{array}{lll}
\text{für } t = 4\alpha & : p = 2t + 1 & = 8\alpha + 1 \\
\text{für } t = 4\alpha + 1 & : p = 2t & = 8\alpha + 2 \\
\text{für } t = 4\alpha + 2 & : p = 2t & = 8\alpha + 4 \\
\text{für } t = 4\alpha + 3 & : p = 2t + 2 & = 8\alpha + 8\,.
\end{array} \qquad (6)
$$

Man beachte, daß es nicht etwa möglich ist, p dadurch zu erhöhen, daß man n in der Form $u2^{t-s} \cdot 2^s$ schreibt und p nach (5) aus s bestimmt.

Schreibt man also n in der Form $n = u \cdot 2^{4\alpha+\beta}$ (u ungerade; $\beta = 0, 1, 2, 3$), so gibt es dann und nur dann $p - 1$ (bzw. p) orthogonale n-reihige Matrizen, die den Gleichungen (2) (*bzw.* (1)) *genügen, wenn $p \leqslant 8\alpha + 2^\beta$ ist; man kann sie sogar reell wählen.*

Das ist aber die Behauptung, wie sie Radon [2] formuliert hat. — Genügt p dieser Bedingung, so gibt es, wie man dem Nachsatz zu (4)

[6]) Statt den angegebenen Zahlen p ist bei gleichem n natürlich auch jede kleinere Zahl p zulässig; man kann dies auch den Formeln (5) entnehmen.

entnehmen kann, für $p \not\equiv 0 \pmod{4}$ bis auf Äquivalenz genau eine Lösung, für $p \equiv 0 \pmod{4}$ dagegen $m+1$ verschiedene, wobei m die Anzahl der irreduziblen orthogonalen Bestandteile bedeutet, also

$$m = \frac{n}{2^{\frac{p-2}{2}}} \quad \text{für } p \equiv 0 \ (\text{mod. } 8)\ ,$$

$$m = \frac{n}{2^{\frac{p}{2}}} \quad \text{für } p \equiv 4 \ (\text{mod. } 8)\ .$$

(Eingegangen den 3. März 1943.)

LITERATUR

[1] *A. Hurwitz*, Über die Komposition der quadratischen Formen, Math. Ann. Bd. 88 (1923), 1—25 (Math. Werke II, 641—666; Seitenangaben in unserem Text beziehen sich auf den Abdruck in den Math. Werken).

[2] *J. Radon*, Lineare Scharen orthogonaler Matrizen, Abh. Sem. Hamburg I (1923), 1—14.

[3] *A. Hurwitz*, Über die Komposition quadratischer Formen von beliebig vielen Variabeln, Nachr. Ges. d. Wiss. Göttingen (1898), 309—316 (Math. Werke II, 565—571).

[4] *P. Jordan*, *J. v. Neumann*, *E. Wigner*, On algebraic generalization of the quantum mechanic formalism, Ann. of Math. 35 (1934), 29—64, insbes. S. 51 bis 54.

[5] *G. Frobenius* und *J. Schur*, Über die reellen Darstellungen der endlichen Gruppen, Sitzungsber. preuß. Akad. d. Wiss. 1906, 186—208.