



Journal für die reine und angewandte Mathematik

Herausgegeben von **Helmut Hasse**

Druck und Verlag Walter de Gruyter & Co., Berlin W 35

Sonderabdruck aus Band 177 Heft 4. 1937.

Über die Galoissche Gruppe der Hermiteschen Polynome.

Von *Werner Schulz* in Berlin.

Über die Galoissche Gruppe der Hermiteschen Polynome.

Von Werner Schulz in Berlin.

In der vorliegenden Arbeit soll gezeigt werden, daß folgende von Herrn I. Schur ausgesprochene und für $n > 12$ bewiesene Vermutung¹⁾ auch für $n \leq 12$ richtig ist:

Satz. *Bedeutet*

$$H_m(x) = (-1)^m e^{\frac{x^2}{2}} \frac{d^m}{dx^m} \left(e^{-\frac{x^2}{2}} \right) = \sum_{\mu=0}^{\left[\frac{m}{2} \right]} (-1)^\mu \binom{m}{2\mu} 1 \cdot 3 \cdot 5 \cdots (2\mu - 1) x^{m-2\mu}$$

das m -te Hermitesche Polynom und setzt man

$$H_{2n}(x) = K_n^{(0)}(x^2), \quad H_{2n+1}(x) = x K_n^{(1)}(x^2),$$

so ist die Galoissche Gruppe der Gleichungen

$$K_n^{(\varepsilon)}(x) = 0 \quad (\varepsilon = 0, 1)$$

die symmetrische Gruppe $\mathfrak{S}_n$.

§ 1. Hilfsmittel für den Beweis.

Bei den Schurschen Untersuchungen spielt folgendes Kriterium eine wichtige Rolle:

Es liege eine Gleichung n -ten Grades $F(x) = 0$ mit ganzen rationalen Koeffizienten vor, die folgende Bedingungen erfüllt:

- a) Die Funktion $F(x)$ ist im Körper der rationalen Zahlen irreduzibel.
- b) Die Diskriminante der Gleichung $F(x) = 0$ enthält eine Primzahl p mindestens in der n -ten Potenz.
- c) Das konstante Glied von $F(x)$ ist durch p , aber nicht durch p^2 teilbar.
- d) Es gilt eine Kongruenz der Form

$$F(x) \equiv x^k f(x) \pmod{p} \quad (k > 1),$$

wobei die Diskriminante des Polynoms $f(x)$ zu p teilerfremd ist.

Dann besitzt die Galoissche Gruppe der Gleichung eine durch p teilbare Ordnung.

Mit Hilfe dieses Kriteriums gelingt es zu zeigen, daß die Ordnung $g_n^{(\varepsilon)}$ der Galoisschen Gruppe $\mathfrak{G}_n^{(\varepsilon)}$ von $K_n^{(\varepsilon)}(x) = 0$ durch jede Primzahl p des Intervalls

$$\frac{2n + 2\varepsilon}{3} < p < n$$

¹⁾ I. Schur, Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome, dieses Journal 165 (1931), S. 52–58.

teilbar sein muß.

Da nun eine Gruppe des Grades n , in deren Ordnung eine Primzahl p des Intervalls

$$\frac{n}{2} < p < n - 2$$

aufgeht, die alternierende oder symmetrische Gruppe n -ten Grades ist, so umfaßt $\mathfrak{G}_n^{(e)}$ die alternierende Gruppe $\mathfrak{A}_n$, sobald eine Primzahl p mit

$$\frac{2n + 2\varepsilon}{3} < p < n - 2$$

existiert. Dies trifft für alle $n > 13$ mit Ausnahme von $n = 19$, $\varepsilon = 1$ zu. So erkennt man für diese Fälle die Affektlosigkeit der Gleichungen $K_n^{(e)}(x) = 0$, wenn man noch beachtet, daß die Diskriminante

$$(1) \quad \Delta_n^{(e)} = 2^{\frac{n(n-1)}{2}} \cdot 2^2 \cdot 3^3 \cdots n^n (3 + 2\varepsilon) (5 + 2\varepsilon)^2 \cdots (2n - 1 + 2\varepsilon)^{n-1}$$

von $K_n^{(e)}(x)$ keine Quadratzahl ist ²⁾.

Für die kleinen Werte von n lassen sich die beim Beweis benötigten Primzahlbedingungen nicht mehr verwirklichen. Man hat hier die Möglichkeit, Permutationen aus $\mathfrak{G}_n^{(e)}$ zu finden, wenn man folgenden Satz von Dedekind heranzieht:

Ist $F(x)$ ein Polynom mit ganzen rationalen Koeffizienten und dem höchsten Koeffizienten 1 und gilt für eine Primzahl p die Zerlegung

$$F(x) \equiv F_1(x) F_2(x) \cdots F_r(x) \pmod{p},$$

wobei die Faktoren $F_i(x) \pmod{p}$ irreduzibel und untereinander inkongruent sind, so enthält die Galoissche Gruppe der Gleichung $F(x) = 0$ eine Permutation, die in r Zyklen zerfällt, deren Ordnungen die Gradzahlen der $F_i(x)$ sind.

Dieser Satz kann zur Bestimmung der Galoisschen Gruppe benutzt werden in Verbindung mit dem folgenden:

Eine primitive Gruppe $\mathfrak{G}$ des Grades n , die einen Zyklus der Primzahlordnung q enthält, ist mindestens $(n - q + 1)$ -fach transitiv. Ist $q = 2$, so ist $\mathfrak{G} = \mathfrak{S}_n$; für $q = 3$ muß $\mathfrak{A}_n$ in $\mathfrak{G}$ liegen.

Für die praktische Anwendung des Dedekindschen Satzes im Fall der Gleichungen $K_n^{(e)}(x) = 0$ ergeben sich einige Unannehmlichkeiten. Zunächst sind die kleinen Primzahlen für die Benutzung unbrauchbar; denn ein Primzahlmodul, für den der Satz anwendbar sein soll, darf nicht in der Diskriminante der Gleichung aufgehen, muß also im vorliegenden Fall nach (1) größer als $2n - 1 + 2\varepsilon$ sein. Ferner kommt hinzu, daß das Auffinden eines irreduziblen Faktors von $K_n^{(e)}(x) \pmod{p}$, der nicht linear oder quadratisch ist, mit einem recht erheblichen Rechenaufwand verbunden sein kann.

Diese Schwierigkeiten für die Bestimmung von $\mathfrak{G}_n^{(e)}$ in den bei Herrn Schur nicht erledigten Fällen lassen sich nun beheben, wenn man eine Verschärfung des Schurschen Kriteriums benutzt, die ich in meiner Dissertation aufgestellt habe ³⁾:

Es liege eine Gleichung n -ten Grades $F(x) = 0$ mit ganzen rationalen Koeffizienten vor, die folgende Bedingungen erfüllt:

- a) $F(x)$ ist im Körper der rationalen Zahlen irreduzibel.
- b) Das konstante Glied von $F(x)$ enthält eine Primzahl p genau im Quadrat.

²⁾ Die in dieser Arbeit als bekannt angegebenen Tatsachen über $K_n^{(e)}(x)$ sind bei Herrn Schur a. a. O. ¹⁾ bewiesen.

³⁾ Werner Schulz, Reduzibilität, Irreduzibilität und Affektfreiheit bei gewissen Klassen von Polynomen, Schriften d. Math. Seminars u. d. Inst. f. angew. Math. d. Universität Berlin **3** (1937), S. 117—154, insbes. S. 138—140.

c) Es gilt

$$F(x) \equiv x^k \psi(x) \pmod{p} \quad (k > 1),$$

wobei die Diskriminante von $\psi(x)$ zu p teilerfremd ist.

d) Es gilt

$$F(x) \equiv x^l \chi(x) \pmod{p^2} \quad \left(l < \frac{k}{2}\right),$$

wobei $\chi(x) \not\equiv 0 \pmod{p^2, x}$ ist.

e) Die Diskriminante von $F(x)$ enthält p mindestens in der $(n + 2l)$ -ten Potenz. Dann besitzt die Galoissche Gruppe der Gleichung eine durch p teilbare Ordnung.

Mit diesem Kriterium kann man für einen Teil der bisher offen gelassenen Fälle die Richtigkeit des eingangs genannten Satzes nachweisen, für die restlichen Fälle liefert der Dedekindsche Satz das gesuchte Ergebnis.

§ 2. Ein Hilfssatz über die Primteiler von $g_n^{(\varepsilon)}$.

Hilfssatz. Die Ordnung $g_n^{(\varepsilon)}$ der Galoisschen Gruppe $\mathfrak{G}_n^{(\varepsilon)}$ von $K_n^{(\varepsilon)}(x) = 0$ ist durch jede Primzahl p des Intervalls

$$(2) \quad \frac{n+2}{2} \leq p \leq \frac{2n-1+2\varepsilon}{3} \quad (p > 3)$$

teilbar. (Außerdem ist bekannt (vgl. § 1), daß $g_n^{(\varepsilon)}$ durch jede Primzahl des Intervalls $\frac{2n+2\varepsilon}{3} < p < n$ teilbar ist.)

Beweis. Es soll gezeigt werden, daß für jedes p aus (2) die Voraussetzungen a) bis e) des im vorigen Paragraphen zuletzt genannten Kriteriums zutreffen. Dann ist die Richtigkeit des Hilfssatzes sichergestellt.

$K_n^{(\varepsilon)}(x)$ ist bekanntlich im Körper der rationalen Zahlen irreduzibel; somit gilt a).

Für die übrigen Bedingungen des Kriteriums ist festzustellen, in welcher Potenz p in den Koeffizienten von $K_n^{(\varepsilon)}(x)$ auftritt. Der Koeffizient von $x^{n-\nu}$ in $K_n^{(\varepsilon)}(x)$ ist

$$(3) \quad a_\nu^{(\varepsilon)} = (-1)^\nu \binom{2n+\varepsilon}{2\nu} 1 \cdot 3 \cdot 5 \cdots (2\nu-1) = \frac{(-1)^\nu}{2^\nu} \frac{(2n+\varepsilon)!}{(2n-2\nu+\varepsilon)! \nu!}.$$

Die höchste Potenz von p , die in $a_\nu^{(\varepsilon)}$ aufgeht, sei $t_\nu^{(\varepsilon)}$. Dann wird behauptet:

$$(4) \quad t_\nu^{(\varepsilon)} = 0 \quad \text{für} \quad \nu = n - \frac{3p+1-2\varepsilon}{2},$$

$$(5) \quad t_\nu^{(\varepsilon)} \geq 1 \quad \text{für} \quad n - \frac{3p+1-2\varepsilon}{2} < \nu < n - \frac{p+1-2\varepsilon}{2},$$

$$(6) \quad t_\nu^{(\varepsilon)} = 1 \quad \text{für} \quad \nu = n - \frac{p+1-2\varepsilon}{2},$$

$$(7) \quad t_\nu^{(\varepsilon)} = 2 \quad \text{für} \quad n - \frac{p+1-2\varepsilon}{2} < \nu \leq n.$$

Für $\nu = n - \frac{3p+1-2\varepsilon}{2}$ folgt nämlich aus (2)

$$(8) \quad \begin{aligned} 3p &\leq 2n + \varepsilon < 4p, \\ 3p &\leq 2n - 2\nu + \varepsilon = 3p + 1 - \varepsilon < 4p, \\ 0 &\leq \nu = n - \frac{3p+1-2\varepsilon}{2} < p. \end{aligned}$$

Folglich geht p wegen (3) in dem zugehörigen $a_\nu^{(\varepsilon)}$ nicht auf, d. h. es gilt (4).

Ist $\nu = n - \frac{3p+1-2\varepsilon}{2} + \delta$ ($\delta = 1, 2, \dots, p$), so bestehen außer (8) die Ungleichungen

$$p \leq 2n - 2\nu + \varepsilon = 3p + 1 - \varepsilon - 2\delta < 3p,$$

$$0 < \nu = n - \frac{3p+1-2\varepsilon}{2} + \delta < 2p.$$

Man unterscheide nun, was nach (2) möglich ist:

$$\alpha) \quad \delta \leq \frac{p+1-\varepsilon}{2}. \quad \text{Dann ist } t_v^{(e)} = 1.$$

$$\beta) \quad \frac{p+1-\varepsilon}{2} < \delta < \frac{5p-2n+1-2\varepsilon}{2}. \quad \text{Dann ist } t_v^{(e)} = 2.$$

$$\gamma) \quad \delta \geq \frac{5p-2n+1-2\varepsilon}{2}. \quad \text{Dann ist } t_v^{(e)} = 1.$$

Das zeigt die Richtigkeit von (5) und (6).

Ist $\nu = n - \frac{p+1-2\varepsilon}{2} + \delta$ ($\delta = 1, 2, \dots, \frac{p+1-2\varepsilon}{2}$), so gilt außer (8)

$$0 \leq 2n - 2\nu + \varepsilon = p + 1 - \varepsilon - 2\delta < p,$$

$$p < \nu = n - \frac{p+1-2\varepsilon}{2} + \delta < 2p.$$

Hieraus folgt (7), und insbesondere erkennt man die Gültigkeit von b).

Aus (4), (5), (6) und (7) ergibt sich

$$K_n^{(e)}(x) \equiv x^{\frac{3p+1-2\varepsilon}{2}} \psi^{(e)}(x) \pmod{p}.$$

Eine einfache Rechnung lehrt ferner, daß

$$\psi^{(0)}(x) \equiv K_{n-\frac{3p+1}{2}}^{(1)}(x) \pmod{p},$$

$$\psi^{(1)}(x) \equiv K_{n-\frac{3p-1}{2}}^{(0)}(x) \pmod{p}$$

ist. Nun ist die Diskriminante $\Delta_n^{(e)}$ von $K_n^{(e)}(x)$ nach (1) nur durch Primzahlen teilbar, die nicht größer als $2n - 1 + 2\varepsilon$ sind. Da wegen (2)

$$p \geq 2n - 3p + 4$$

ist, so wird die Diskriminante von $\psi^{(e)}(x)$ zu p teilerfremd. Also besteht c) mit $k = \frac{3p+1-2\varepsilon}{2} > 1$.

Weiter ist

$$K_n^{(e)}(x) \equiv x^{\frac{p+1-2\varepsilon}{2}} \chi^{(e)}(x) \pmod{p^2},$$

wo $\chi^{(e)}(x) \not\equiv 0 \pmod{p^2, x}$ ist, d. h. es gilt d) mit $l = \frac{p+1-2\varepsilon}{2} < \frac{k}{2}$.

In $\Delta_n^{(e)}$ treten wegen (2) die Faktoren p^p , $p^{\frac{p-1-2\varepsilon}{2}}$ und $(3p)^{\frac{3p-1-2\varepsilon}{2}}$ auf. Da

$$p + \frac{p-1-2\varepsilon}{2} + \frac{3p-1-2\varepsilon}{2} = 3p - 1 - 2\varepsilon \geq n + 2 + p - 1 - 2\varepsilon = n + 2l$$

ist, so ist auch e) erfüllt.

§ 3. Beweis des Satzes für $n \leq 12$.

Die Gruppe $\mathfrak{G}_n^{(\varepsilon)}$ ist transitiv und kann nicht $\mathfrak{A}_n$ sein, da $\Delta_n^{(\varepsilon)}$ keine Quadratzahl ist. Es ist also zu beweisen, daß $\mathfrak{A}_n$ in $\mathfrak{G}_n^{(\varepsilon)}$ enthalten ist.

$n = 2$ und 3 . Hier ist die Richtigkeit der Behauptung trivial.

$n = 4$. Es ist $g_4^{(0)} \equiv 0 \pmod{3}$, was auf $\mathfrak{A}_4 < \mathfrak{G}_4^{(0)}$ führt. Für $\varepsilon = 1$ ist man auf den Dedekindschen Satz angewiesen. Da in der Zerlegung

$$K_4^{(1)}(x) \equiv (x-5)(x^3 + 2x^2 + 3x - 2) \pmod{11}$$

die Faktoren mod 11 irreduzibel sind, so muß $\mathfrak{G}_4^{(1)}$ einen Dreierzyklus und somit $\mathfrak{A}_4$ enthalten.

$n = 5$. Auch hier kann noch nicht der Hilfssatz benutzt werden, da in dem Intervall $\frac{5+2}{2} \leq p < 5$ keine Primzahl vorhanden ist. $\mathfrak{G}_5^{(\varepsilon)}$ ist als Gruppe von Primzahlgrad primitiv und enthält einen Dreierzyklus, da in den Zerlegungen

$$K_5^{(0)}(x) \equiv (x-6)(x+7)(x^3 + 5x^2 + 4x - 3) \pmod{17},$$

$$K_5^{(1)}(x) \equiv (x-1)(x+6)(x^3 + 5x^2 - 4x - 3) \pmod{13}$$

die Faktoren irreduzibel sind. Also ist $\mathfrak{A}_5 < \mathfrak{G}_5^{(\varepsilon)}$.

$n = 6$. Es ist $g_6^{(\varepsilon)} \equiv 0 \pmod{5}$, was die Primitivität von $\mathfrak{G}_6^{(\varepsilon)}$ nach sich zieht. Ferner bestehen folgende Zerlegungen in irreduzible Bestandteile:

$$K_6^{(0)}(x) \equiv (x+13)(x^2 + 8x - 7)(x^3 + 6x^2 - 9x + 5) \pmod{31},$$

$$K_6^{(1)}(x) \equiv (x-4)(x^2 + 9x + 7)(x^3 - 7x^2 + 5x - 5) \pmod{19}.$$

Da $\mathfrak{G}_6^{(\varepsilon)}$ hiernach eine Permutation der Form $(\alpha_1, \alpha_2)(\beta_1, \beta_2, \beta_3)$, also auch eine Transposition enthält, so ist $\mathfrak{G}_6^{(\varepsilon)} = \mathfrak{S}_6$.

$n = 7$ und 8 . Auf Grund des Hilfssatzes ist $g_n^{(\varepsilon)} \equiv 0 \pmod{5}$, und daher muß $\mathfrak{A}_n < \mathfrak{G}_n^{(\varepsilon)}$ sein.

$n = 9$. Es ist $g_9^{(\varepsilon)} \equiv 0 \pmod{7}$, woraus die Primitivität von $\mathfrak{G}_9^{(\varepsilon)}$ folgt. Ferner gilt

$$K_9^{(0)}(x) \equiv (x-3)(x+11)(x^2 + 18x + 11)(x^5 + 9x^4 - 12x^3 + 17x^2 - 19x - 19) \pmod{47},$$

$$K_9^{(1)}(x) \equiv (x-5)(x-17)(x^2 + 33x - 17)(x^5 + 19x^4 + 17x^3 + 2x^2 + 6x + 26) \pmod{67}.$$

In beiden Zerlegungen kommt kein weiterer Linearfaktor vor; dagegen könnten die Faktoren fünften Grades noch in einen quadratischen und kubischen Faktor zerfallen. In jedem Fall enthält $\mathfrak{G}_9^{(\varepsilon)}$ eine Permutation, von der eine geeignete Potenz eine Transposition oder einen Dreierzyklus liefert. Somit ist $\mathfrak{A}_9 < \mathfrak{G}_9^{(\varepsilon)}$.

$n = 10, 11, 12$. Nach dem Hilfssatz ist $g_n^{(\varepsilon)} \equiv 0 \pmod{7}$ und folglich $\mathfrak{A}_n < \mathfrak{G}_n^{(\varepsilon)}$.

Auch der bei Herrn Schur nur unter Benutzung genauerer Ergebnisse über die möglichen primitiven Permutationsgruppen des Grades 18 bewiesene Fall $n = 19$, $\varepsilon = 1$ ist nach dem Hilfssatz wegen $g_{19}^{(1)} \equiv 0 \pmod{13}$ sofort zu erledigen.