Compositio Mathematica

Friedrich Levi

Zur Irreduzibilität der Kreisteilungspolynome

Compositio Mathematica, tome 1 (1935), p. 303-304
<http://www.numdam.org/item?id=CM_1935__1__303_0>

© Foundation Compositio Mathematica, 1935, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (http://http://www.compositio.nl/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Zur Irreduzibilität der Kreisteilungspolynome

von

Friedrich Levi

Leipzig

Es gibt viele schöne und auch kurze Beweise [1]) dafür, daß im Körper P_0 der rationalen Zahlen jedes Kreisteilungspolynom irreduzibel ist. Bekanntlich gilt diese Irreduzibilität nicht immer in den endlichen Primkörpern P_p. Sie ist also keine unmittelbare Folge davon, daß die Wurzeln multiplikativ eine zyklische Gruppe bilden, sondern sie hängt wesentlich mit der Struktur von P_0 zusammen. Der nachstehende Beweis gestattet einen direkten Einblick, warum P_0 vor den Körpern P_p in dieser Weise ausgezeichnet ist.

Offenbar genügt es folgenden Satz zu beweisen:

Ist α eine primitive m^{te} Einheitswurzel, p zu m teilerfremd, $f(x)$ ein irreduzibeles Polynom mit ganzen rationalen Koeffizienten und $f(\alpha)=0$, so ist auch $f(\alpha^p)=0$.

Beweis: Es sei β eine primitive Wurzel des m^{ten} Kreisteilungspolynoms von P_p. Der Körper $\mathsf{P}_p(\beta)$ ist dann ein homomorphes Bild des Ideals der ganzen Zahlen aus $\mathsf{P}_0(\alpha)$. In $\mathsf{P}_p(\beta)$ gibt es m verschiedene m^{te} Einheitswurzeln. Deshalb vermittelt der Homomorphismus eine ein-eindeutige Abbildung der m^{ten} Einheitswurzeln von $\mathsf{P}_0(\alpha)$ auf die von $\mathsf{P}_p(\beta)$. O. E. d. A. kann man annehmen, daß sich dabei α und β, mithin auch α^i und β^i entsprechen. $f(x)$ wird homomorph auf $g(x)$ abgebildet. Die Wurzeln von $f(x)$ sind Einheitswurzeln $\alpha, \alpha^{r_1}, \ldots, \alpha^{r_s}$; die von $g(x)$ sind dann $\beta, \beta^{r_1}, \ldots, \beta^{r_s}$. Nun erzeugt aber das Potenzieren mit p einen Automorphismus in $\mathsf{P}_p(\beta)$; also ist $g(\beta^p)=0$; daher ist p ein r_i und $f(\alpha^p)=0$.

---

[1]) Eine Zusammenstellung der älteren Beweise (Gauß, Kronecker, Schönemann, Eisenstein, Arndt, Lebesgue, Gravelaar, Dedekind, Kummer, Weber) bei M. Ruthinger, Die Irreduzibilitätsbeweise der Kreisteilungsgleichung [Inaug. Diss. Straßburg 1907]. Ferner ist besonders zu erwähnen: Mertens [Wiener Ber. **114** (1905), 1293—1296; **117** (1908) 689—690], sowie die Beweise von E. Landau und I. Schur [Math. Z. **29** (1929), 462, 463].

Zusätzliche Bemerkungen: 1). Eliminiert man aus dem obigen Beweis den Begriff des endlichen Körpers und fügt die dadurch nötig gewordenen Hilfsbetrachtungen ein, so kommt man zum Beweis von Dedekind [2]). 2). Das achte Kreisteilungspolynom ist in jedem P_p $(p \neq 2)$ in zwei irreduzibele quadratische Faktoren zerlegbar. Die Exponenten 1, 3, 5, 7 der primitiven Wurzeln werden durch diese Faktorzerlegung in je zwei Paare eingeteilt, und zwar treten die drei möglichen Paarungen schon in den drei einfachsten Fällen $p = 3, 5, 7$ auf. Allgemein ist das m^{te} Kreisteilungspolynom in P_p dann und nur dann irreduzibel, wenn p ein primitive Kongruenzwurzel von $x^{\varphi(m)} \equiv 1 \pmod{m}$ ist. Gibt es eine primitive Wurzel dieser Kongruenz, so gibt es auch eine zu ihr kongruente Primzahl p, und das m^{te} Kreisteilungspolynom ist in P_p irreduzibel. Für die Existenz einer primitiven Kongruenzwurzel ist notwendig und hinreichend, daß die Gruppe der Kongruenzwurzeln zyklisch ist. Das ist dann und nur dann der Fall, wenn $m = 4$ oder Potenz einer ungeraden Primzahl oder das Doppelte davon ist.

(Eingegangen den 20. Dezember 1933.)

---

[2]) Beweis für die Irreduktibilität der Kreisteilungsgleichungen [J. f. M. 54 (1857), 27—30].