

# 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](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://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). 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 <sup>1)</sup> dafür, daß im Körper  $\mathbb{P}_0$  der rationalen Zahlen jedes Kreisteilungspolynom irreduzibel ist. Bekanntlich gilt diese Irreduzibilität nicht immer in den endlichen Primkörpern  $\mathbb{P}_p$ . Sie ist also keine unmittelbare Folge davon, daß die Wurzeln multiplikativ eine zyklische Gruppe bilden, sondern sie hängt wesentlich mit der Struktur von  $\mathbb{P}_0$  zusammen. Der nachstehende Beweis gestattet einen direkten Einblick, warum  $\mathbb{P}_0$  vor den Körpern  $\mathbb{P}_p$  in dieser Weise ausgezeichnet ist.

Offenbar genügt es folgenden Satz zu beweisen:

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

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

---

<sup>1)</sup> 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 <sup>2)</sup>. 2). Das achte Kreisteilungspolynom ist in jedem  $\mathbb{P}_p$  ( $p \neq 2$ ) in zwei irreduzible 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  $m^{\text{te}}$  Kreisteilungspolynom in  $\mathbb{P}_p$  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  $m^{\text{te}}$  Kreisteilungspolynom ist in  $\mathbb{P}_p$  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.)

---

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

---