VI.

Beweis für die Irreduktibilität der Kreisteilungs-Gleichungen.

[Journal für reine und angewandte Mathematik, Bd. 54, S. 27—30 (1857)].

Nachdem Gauß[*)] zuerst die Irreduktibilität der Gleichung $\frac{x^p - 1}{x - 1} = 0$ für den Fall bewiesen hatte, daß p eine Primzahl ist, lag es nahe, einen ähnlichen Satz zu vermuten, welcher sich auf die Teilung des Kreisumfangs in eine beliebige Anzahl m gleicher Teile bezieht. Dieser Satz wird so lauten:

„Die Gleichung vom Grade $\varphi(m)$, welche sämtliche $\varphi(m)$ primitive Wurzeln der Gleichung $x^m = 1$ zu Wurzeln hat, ist irreduktibel."

Dem Beweis von Gauß folgte zunächst eine Reihe anderer von Kronecker, Schönemann, Eisenstein, die auf wesentlich verschiedenen Prinzipien beruhen, sich aber sämtlich auf denselben einfachsten Fall beziehen, in welchem m eine Primzahl ist. Doch sieht man leicht, daß diese Prinzipien auch noch auf den Fall anwendbar sind, in welchem m nur durch eine einzige Primzahl teilbar, also eine Potenz dieser Primzahl ist, und namentlich wurden die Beweise von Kronecker und Eisenstein in diesem Sinne von Serret verallgemeinert. Allein diese Prinzipien reichen nicht mehr aus, sobald die Zahl m durch mehrere Primzahlen teilbar ist, weil dann die in Rede stehende Gleichung in verschiedener Hinsicht einen wesentlich anderen Charakter annimmt. Auf diesen Punkt hat zuerst Kronecker[**)] in einer Abhandlung aufmerksam gemacht, welche zugleich den ersten Beweis des obigen, und zwar noch verallgemeinerten Theorems enthält. Obgleich nun dieser Satz für die algebraische Auflösung der Gleichung $x^m = 1$ nicht gerade erforderlich ist, da diese bekanntlich immer auf den Fall zurückgeführt werden kann, in welchem m die Potenz einer einzigen Primzahl ist, so verdient doch vielleicht

[*) Ein vollständiges Literaturverzeichnis über die verschiedenen Beweise für die Irreduzibilität der Kreisteilungsgleichung findet man in: Dickson, Mitchell, Vandiver, Wahlin, Algebraic numbers § 13. Bulletin of the National Research Council, Vol. 5, part 3, no. 28 (1923)].

[**) L. Kronecker, Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$. Journ. de Math. Bd. 19, S. 177—192 (1854)].

ein neuer Beweis desselben, der sich durch seine Einfachheit auszeichnet, die Aufmerksamkeit derjenigen Mathematiker, welche sich mit diesem Teile der Algebra beschäftigen.

1.

Der neue Beweis stützt sich auf elementare Sätze über die Kongruenzen höherer Grade, und ich werde mich in dieser Beziehung auf den vorstehenden Aufsatz über die Theorie derselben berufen; außerdem benutze ich noch den folgenden zuerst von Schönemann [*)] bewiesenen Satz: Ist

$$f(x) = (x - \alpha)(x - \beta) \cdots (x - \lambda)$$

eine ganze rationale Funktion mit reellen ganzzahligen Koeffizienten, p eine absolute Primzahl und

$$f_1(x) = (x - \alpha^p)(x - \beta^p) \cdots (x - \lambda^p),$$

so sind die Koeffizienten dieser letzteren Funktion ebenfalls ganze reelle Zahlen, und zwar den entsprechenden Koeffizienten von $f(x)$ kongruent nach dem Modulus p, in Zeichen

$$f_1(x) \equiv f(x) \pmod{p}.$$

Für den direkten Beweis dieses Satzes, welcher eigentlich nur eine sehr spezielle algebraische Anwendung der genannten Theorie der höheren Kongruenzen ist, mag hier folgende Bemerkung genügen. Sieht man $\alpha, \beta, \ldots, \lambda$ als ganz unbestimmte Größen an und bezeichnet mit A und A_1 irgend zwei einander entsprechende Koeffizienten der beiden Funktionen $f(x)$ und $f_1(x)$, so leuchtet ein, daß man $A^p = A_1 + pA_2$ setzen kann, worin A_1 und A_2 ganze, ganzzahlige und zugleich symmetrische Funktionen von $\alpha, \beta, \ldots, \lambda$ und folglich auch (nach dem Fundamentalsatze über die Transformation symmetrischer Funktionen) ganze und ganzzahlige Funktionen der Koeffizienten A von $f(x)$ sind. Sind daher diese Koeffizienten ganze reelle Zahlen, so erhält man $A^p \equiv A_1 \pmod{p}$, und nach dem Fermatschen Satze also auch $A \equiv A_1 \pmod{p}$, was zu beweisen war.

2.

Es sei nun α irgend eine primitive Wurzel der Gleichung $x^m = 1$ und $f(x)$ der durch $x - \alpha$ teilbare irreduktibele Faktor von $x^m - 1$, dessen rationale Koeffizienten sämtlich ganze Zahlen sein müssen,

[*) Th. Schönemann, Grundzüge einer allgemeinen Theorie der höheren Kongruenzen, deren Modul eine reelle Primzahl ist; § 13. Journ. f. Math. Bd. 31, S. 269—325 (1846)].

wenn der der höchsten Potenz von x gleich Eins angenommen wird (Disqu. Arithm. Art. 42). Der zu beweisende Satz ist dann identisch mit dem folgenden: „Die Gleichung $f(x) = 0$ hat zu Wurzeln sämtliche $\varphi(m)$ primitive $m$te Wurzeln der Einheit, und keine anderen.“ Der Beweis des letzteren Teiles dieses Satzes hat keine Schwierigkeit, soll aber doch der Vollständigkeit halber hier nicht übergangen werden. Ist α^r irgend eine Wurzel der Gleichung $f(x) = 0$ — und in dieser Form sind ja alle ihre Wurzeln enthalten —, so folgt in bekannter Weise aus der Irreduktibilität von $f(x)$, daß jedes Glied der Reihe α^r, α^{r^2}, α^{r^3}, $\cdots$ eine Wurzel der Gleichung ist, und daß in dieser Reihe früher oder später einmal ein Glied α^{r^n} kommen muß, welches $= \alpha$ ist; daraus folgt aber $r^n \equiv 1 \pmod{m}$, und es ist daher r relative Primzahl gegen m, und folglich α^r ebenfalls eine primitive $m$te Wurzel der Einheit.

Ungleich schwieriger ist der Nachweis des ersten Teiles, daß nämlich umgekehrt jede primitive $m$te Wurzel der Einheit (d. h. jedes α^r, wenn r relative Primzahl gegen m ist) der Gleichung $f(x) = 0$ genügt; doch kann man das Problem sogleich auf den einfachsten Fall reduzieren, in welchem r eine absolute Primzahl ist, die natürlich nicht in m aufgehen darf. Ist nämlich bewiesen, daß α^r, α^s der Gleichung $f(x) = 0$ genügen, so muß auch $\alpha^{r \cdot s}$ ihr genügen; denn da der Annahme nach α der rationalen Gleichung $f(x^r) = 0$ genügt, so muß ihr auch jede andere Wurzel α^s der irreduktibeln Gleichung $f(x) = 0$ genügen. Offenbar braucht also nur noch gezeigt zu werden, daß jedes α^p der Gleichung $f(x) = 0$ genügt, wenn p eine absolute Primzahl ist, welche nicht in m aufgeht.

3.

Um dies zu beweisen, bemerken wir, daß die Wurzeln der irreduktibeln Gleichung $f_1(x) = 0$, welcher α^p genügt, mit den $p$ten Potenzen der Wurzeln der Gleichung $f(x) = 0$ übereinstimmen müssen; denn da α^p ebensowohl eine rationale Funktion von α, wie umgekehrt α von α^p ist (nämlich $= (\alpha^p)^{p'}$, wenn $pp' \equiv 1 \pmod{m}$), so müssen die Grade der beiden Funktionen $f(x)$ und $f_1(x)$ einander gleich sein. Setzt man daher

$$f(x) = (x - \alpha)(x - \beta) \cdots (x - \lambda),$$

so ist

$$f_1(x) = (x - \alpha^p)(x - \beta^p) \cdots (x - \lambda^p)$$

und folglich nach dem oben bewiesenen Satze von Schönemann

$$f_1(x) \equiv f(x) \pmod{p}.$$

Und aus dieser Kongruenz zwischen den beiden Funktionen $f(x)$ und $f_1(x)$ folgt auch ihre Identität. Denn nehmen wir an, die beiden irreduktibeln Funktionen $f(x)$ und $f_1(x)$ sind nicht identisch, so können sie auch keinen gemeinschaftlichen Faktor haben, und folglich ist $x^m - 1$ durch ihr Produkt teilbar, da $x^m - 1$ sowohl durch $f(x)$ als auch durch $f_1(x)$ teilbar ist. Es wäre daher $x^m - 1$ einem Produkt von Faktoren gleich, unter denen mindestens zwei einander nach dem Modulus p kongruent wären. Dann müßte (zufolge Art. 6 des vorstehenden Aufsatzes über die höheren Kongruenzen) die Funktion $x^m - 1$ mit ihrer ersten Derivierten mx^{m-1} nach dem Modulus p gemeinschaftliche Divisoren haben; da aber m nicht durch p teilbar, und folglich mx^{m-1} auch nicht $\equiv 0 \pmod{p}$ ist, so hat mx^{m-1} nach dem Modulus p nur solche primäre Primfaktoren, welche $\equiv x$ sind; und offenbar hat $x^m - 1$ keinen solchen Primfaktor nach dem Modulus p, da sonst für $x \equiv 0$ auch $x^m - 1 \equiv 0$ werden müßte, was ja nicht der Fall ist.

Mithin sind die beiden Funktionen $f(x)$ und $f_1(x)$ identisch; jedes α^p und folglich auch jedes α^r genügt also einer und derselben irreduktibeln Gleichung $f(x) = 0$, wenn r relative Primzahl gegen m ist. W. Z. B. W.

Göttingen, im Oktober 1856.

Erläuterungen zur vorstehenden Abhandlung.

Der vorliegende Dedekindsche Beweis der Irreduzibilität der allgemeinen Kreisteilungsgleichung ist in bezug auf Einfachheit dem S. 68 zitierten Kroneckerschen Beweise überlegen, obwohl die Verallgemeinerung auf die Irreduzibilität in Körpern, deren Diskriminante zu m relativ prim ist, nicht so einfach wird. Der Dedekindsche Beweis ist in H. Weber, Algebra, 2. Aufl. (1898), Bd. 1, S. 596—600 reproduziert.

F. Mertens (Sitzungsber. d. Akad. d. Wiss. in Wien 1905, IIa, S. 1293—96) hat eine Vereinfachung des Dedekindschen Beweises vorgeschlagen, indem er direkt beweist, daß wenn r zu m relativ prim ist, dann $f(x^r)$ algebraisch durch $f(x)$ teilbar sein muß (Bezeichnung von § 2). Das Dedekindsche Prinzip ist auch im Beweise von H. Späth (Math. Zeitschr. Bd. 26, S. 442—444 (1927)) angewandt. Aber die Dedekindsche Vereinfachung, daß r als Primzahl angenommen werden darf, ist von diesen Autoren nicht übernommen.

Ore.
