XL.

Zur Theorie der Ideale (Göttingen 1894). Anwendung auf die Kreiskörper.

Lemma 1. Ist m eine natürliche Zahl, und α eine primitive Wurzel der Gleichung

$$\alpha^m = 1,$$

so ist

$$\alpha - 1 = 0,$$

wenn $m = 1$,

$$(\alpha - 1)^{\varphi(m)} = \varepsilon p,$$

wenn m durch eine und nur eine Primzahl p teilbar ist, und ε eine Einheit bedeutet; $\alpha - 1 = \varepsilon$, wenn m durch mindestens zwei verschiedene Primzahlen teilbar ist.

Beweis. Der erste Fall ist evident. Durchläuft $\alpha' = \alpha^r$ im zweiten Falle alle $\varphi(m)$ primitiven m-ten Einheitswurzeln, und nimmt man $rr' \equiv 1 \pmod{m}$, so sind

$$\frac{\alpha' - 1}{\alpha - 1} = \frac{\alpha^r - 1}{\alpha - 1} \quad \text{und} \quad \frac{\alpha - 1}{\alpha' - 1} = \frac{\alpha'^{r'} - 1}{\alpha' - 1}$$

ganz, also Einheiten, und da

$$\prod(x - \alpha') = \frac{x^m - 1}{x^{\frac{m}{p}} - 1}, \quad \text{also} \quad \prod(1 - \alpha') = p,$$

so folgt das zweite Resultat. Ist endlich $m = pqn$ durch zwei verschiedene Primzahlen p, q teilbar, so ist $\alpha - 1$ gemeinsamer Teiler von $\alpha^{qn} - 1$ und $\alpha^{pn} - 1$, also (nach dem zweiten Fall) gemeinsamer Teiler von p und q, also eine Einheit, w. z. b. w.

Lemma 2. Es sei $\mathfrak{p}$ ein Primideal eines endlichen Körpers Ω, und p die durch $\mathfrak{p}$ teilbare natürliche Primzahl, $N(\mathfrak{p}) = p^f$, wo f der Grad von $\mathfrak{p}$. Ist nun α eine in Ω enthaltene primitive m-te Einheitswurzel, und setzt man $m = m'p'$, wo p' die höchste in m aufgehende Potenz von p ist, so gehört α zum Exponent m' (mod. $\mathfrak{p}$).

Beweis. Ist ω relative Primzahl zu $\mathfrak{p}$ in Ω, so ist

$$\omega^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}},$$

und der Exponent, zu welchem ω gehört (mod. $\mathfrak{p}$), ist die kleinste natürliche Zahl e, welche der Bedingung $\omega^e \equiv 1 \pmod{\mathfrak{p}}$ genügt; dann ist e ein Divisor von $N(\mathfrak{p}) - 1$, also gewiß unteilbar durch p. Wendet man dies auf den Fall $\omega = \alpha$ an, so folgt aus $\alpha^m = \alpha^{m'p'} = 1 \equiv 1 \pmod{\mathfrak{p}}$, daß e Divisor von $m'p'$, also auch von m' ist. Setzt man nun $m' = ee'$, so ist α^e eine primitive $(e'p')$-te Einheitswurzel, und da $\alpha^e - 1 \equiv 0 \pmod{\mathfrak{p}}$, also keine Einheit ist, so sind (nach Lemma 1) nur zwei Fälle möglich: Entweder ist $e'p' = 1$, also $e' = 1$, $e = m' = m$. Oder $e'p'$ ist durch eine und nur eine Primzahl q teilbar; dann ist $\alpha^e - 1$ (nach Lemma 1) Divisor von q, und da $\alpha^e - 1$, also auch q durch $\mathfrak{p}$ teilbar ist, so muß $q = p$ sein; also ist $e'p'$ Potenz von p, und da e' als Divisor von m' nicht durch p teilbar ist, so muß auch in diesem Falle $e' = 1$, $e = m'$ sein. Also ist in beiden Fällen $e = m'$, w. z. b. w.

Zusatz. Da e Divisor von $N(\mathfrak{p}) - 1 = p^f - 1$ ist, so folgt $p^f \equiv 1 \pmod{m'}$.

Lemma 3. Es sei wieder α eine primitive m-te Einheitswurzel, und $\Omega = R(\alpha) = K_m$ der durch α erzeugte Körper. Als bekannt wird nur Folgendes vorausgesetzt. Die sämtlichen $\varphi(m)$ primitiven m-ten Einheitswurzeln $\alpha' = \alpha^r$, wo r alle nach m inkongruenten relativen Primzahlen zu m durchläuft, sind die sämtlichen Wurzeln einer Gleichung vom Grade $\varphi(m)$ mit rationalen Koeffizienten (ihre Irreduzibilität soll erst bewiesen, nicht vorausgesetzt werden). Jedenfalls folgt hieraus, daß alle n mit α konjugierten Zahlen unter diesen Zahlen α' zu suchen sind; durch jede der n entsprechenden Permutationen φ' geht α in eine dieser n Zahlen $\alpha\varphi' = \alpha' = \alpha^{r'}$ über, und da $\Omega' = \Omega\varphi' = R(\alpha') = R(\alpha^{r'})$ offenbar ein Divisor von Ω und folglich (!) auch $= \Omega$ ist, so ist Ω ein Normalkörper. Sind φ', φ'' zwei solche Permutationen von Ω, und zwar $\alpha\varphi' = \alpha^{r'}$, $\alpha\varphi'' = \alpha^{r''}$, so folgt $(\alpha\varphi')\,\varphi'' = (\alpha^{r'})\,\varphi'' = (\alpha\varphi'')^{r'} = (\alpha^{r''})^{r'} = \alpha^{r'r''}$, ebenso $(\alpha\varphi'')\,\varphi' = \alpha^{r''r'}$, mithin $\varphi'\varphi'' = \varphi''\varphi'$, d. h. Ω ist ein Abelscher Körper, und die Gruppe Φ aller n Permutationen φ ist eine Abelsche Gruppe. Man kann eine Permutation φ, durch welche α in $\alpha\varphi = \alpha^r$ übergeht, kurz als Permutation r bezeichnen, wo r ein beliebiger Repräsentant der ganzen Zahlenklasse r (mod. m) ist, und die Zu-

sammensetzung der Permutationen φ in der Gruppe Φ entspricht der Multiplikation dieser Zahlenklassen; die identische Permutation entspricht der Zahlenklasse 1 (mod. m). Diese Gruppe Φ ist dann ein Teiler der aus allen $\varphi(m)$ Klassen bestehenden Gruppe, also ihr Grad n ein Divisor von $\varphi(m)$.

Satz: Es ist $n = \varphi(m)$; d. h. die Gleichung, deren Wurzeln die $\varphi(m)$ primitiven m-ten Einheitswurzeln sind, ist irreduzibel; Φ ist die Gruppe aller $\varphi(m)$ Zahlenklassen r (mod. m), deren Elemente r relative Primzahlen zu m sind.

Beweis. Ist p eine natürliche Primzahl, die nicht in m aufgeht, und $\mathfrak{p}$ irgendein in p aufgehendes Primideal des Körpers Ω, so gibt es [zur Theorie der Ideale] in der Gruppe Φ mindestens eine Permutation ψ_0 von der Art, daß jede ganze Zahl ω in Ω der Kongruenz

$$\omega^p \equiv \omega\,\psi_0 \pmod{\mathfrak{p}}$$

genügt. Wendet man dies auf $\omega = \alpha$ an und setzt

$$\alpha\,\psi_0 = \alpha^{p_0},$$

wo p_0 relative Primzahl zu m, durch welche ψ_0 vollständig definiert ist, so folgt

$$\alpha^p \equiv \alpha^{p_0} \pmod{\mathfrak{p}}.$$

Wendet man hierauf das obige Lemma 2 an, so ist $p' = 1$, $m' = m$ zu setzen, also gehört α (mod. $\mathfrak{p}$) zum Exponent m, mithin ist $p_0 \equiv p$ (mod. m), und folglich $\alpha\,\psi_0 = \alpha^{p_0} = \alpha^p$. Es ist daher α^p konjugiert mit α. Ist nun r eine beliebige relative Primzahl zu m, so kann man immer $r \equiv p_1 p_2 p_3 \cdots$ (mod. m) setzen, wo $p_1, p_2, p_3 \cdots$ natürliche Primzahlen bedeuten; nun gibt es, wie eben gezeigt, immer Permutationen $\varphi_1, \varphi_2, \varphi_3, \cdots$ in der Gruppe Φ, für welche $\alpha\varphi_1 = \alpha^{p_1}$, $\alpha\varphi_2 = \alpha^{p_2}$, $\alpha\varphi_3 = \alpha^{p_3} \cdots$, also auch $\alpha\varphi_1\varphi_2\varphi_3 \cdots = \alpha^{p_1 p_2 p_3 \cdots} = \alpha^r$ wird; mithin ist jede Potenz α^r, d. h. jede primitive m-te Einheitswurzel α' konjugiert mit α, w. z. b. w. (Ähnlichkeit mit meinem Beweise in Crelles Journal Bd. 54).

Erläuterungen zur vorstehenden Abhandlung.

Der hier gegebene Irreduzibilitätsbeweis der Kreisteilungsgleichung beruht auf den beiden Tatsachen:

1. Eine primitive m-te Einheitswurzel bleibt primitiv modulo jedem nicht in m aufgehenden Primideal $\mathfrak{p}$ des Körpers K dieser Einheitswurzeln.

2. Es gibt eine Substitution ψ_0 der Zerlegungsgruppe von $\mathfrak{p}$, für die $\omega\,\psi_0 \equiv \omega^p (\mathfrak{p})$ für jedes ganze ω aus K.

Die vermöge 2. gegebene Zuordnung zwischen Galoisgruppe und Klassengruppe — aus der die Irreduzibilität unmittelbar folgt — ist die Zuordnung im Sinn des allgemeinen Artinschen Reziprozitätsgesetzes, aber in stark abgeschwächter und daher elementarer Form. Denn die Zuordnung geschieht nur zu allen Primzahlen enthaltenden Klassen, also zu einem Erzeugendensystem der Klassengruppe, was zur Festlegung des ganzen Isomorphismus hier ausreicht. Die Frage, ob dieses Erzeugendensystem die Klassengruppe erschöpft, also der Satz von der arithmetischen Progression, bleibt unberührt.

Daß auch die Irreduzibilität der Valenzgleichung in der Theorie der komplexen Multiplikation sich entsprechend beweisen läßt, hat Dedekind an anderer Stelle ohne Beweis-Ausführung bemerkt. Es handelt sich wohl wesentlich um den in Weber, Algebra, Bd. 3, § 122 (2. Auflage) übergegangenen Beweis für die Irreduzibilität der Klassengleichung.

Noether.