XLIII.

Untersuchung der Gruppe X.

(Einige Sätze aus der Untersuchung der Beziehungen zwischen den Idealen in verschiedenen Körpern. Schreiben an G. Frobenius vom 8. Juni 1882.)

Es sei χ eine nicht identische Permutation der Gruppe X (also $g > 1$), und $\mathfrak{p}^r$ die höchste in allen Differenzen $\omega\chi - \omega$ aufgehende Potenz von $\mathfrak{p}$, also

$$\omega\chi \equiv \omega \pmod{\mathfrak{p}^r},$$

aber nicht identisch

$$\omega\chi \equiv \omega \pmod{\mathfrak{p}^{r+1}}, \quad r \geqq 1.$$

Dann sei $\mathfrak{o}_1$ das System aller derjenigen Zahlen ω_1 in $\mathfrak{o}$, welche die Kongruenz

$$\omega_1\chi \equiv \omega_1 \pmod{\mathfrak{p}^{r+1}}$$

erfüllen. Zunächst leuchtet ein, daß $\mathfrak{o}_1$ ein Modul ist, weil aus $\alpha\chi \equiv \alpha$, $\beta\chi \equiv \beta \pmod{\mathfrak{p}^{r+1}}$ auch $(\alpha - \beta)\chi = \alpha\chi - \beta\chi \equiv \alpha - \beta \pmod{\mathfrak{p}^{r+1}}$ folgt, und zwar ist $\mathfrak{o}_1$ ein echtes Vielfaches von $\mathfrak{o}$, weil $\mathfrak{o}$ nicht teilbar durch $\mathfrak{o}_1$ ist. Da ferner $\mathfrak{p}\chi = \mathfrak{p}$, also auch $\mathfrak{p}^{r+1}\chi = \mathfrak{p}^{r+1}$ ist, so genügt jede in $\mathfrak{p}^{r+1}$ enthaltene Zahl π_{r+1}, weil $\pi_{r+1}\chi = \pi'_{r+1}$ ebenfalls in $\mathfrak{p}^{r+1}$ enthalten ist, der Kongruenz $\pi_{r+1}\chi \equiv \pi_{r+1} \pmod{\mathfrak{p}^{r+1}}$, weil $\pi'_{r+1} \equiv \pi_{r+1} \equiv 0 \pmod{\mathfrak{p}^{r+1}}$ ist; mithin ist $\mathfrak{p}^{r+1}$ teilbar durch $\mathfrak{o}_1$, und folglich enthält $\mathfrak{o}_1$ auch n voneinander unabhängige Zahlen; $\mathfrak{o}_1$ ist ein endlicher n-gliedriger Modul, dessen Basis zugleich eine Basis des Körpers Ω ist. Da $\mathfrak{o} < \mathfrak{o}_1 < \mathfrak{p}^{r+1}$, so ist

$$(\mathfrak{o}, \mathfrak{p}^{r+1}) = p^{(r+1)f} = (\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{p}^{r+1}),$$

also

$$(\mathfrak{o}, \mathfrak{o}_1) = p^h, \quad 0 < h \leqq (r+1)f.$$

Sodann leuchtet ein, daß $\mathfrak{o}_1$ eine Ordnung ist; denn für jede ganze rationale, d. h. in $\mathfrak{z}$ enthaltene Zahl z ist $z\chi = z$, also ist $\mathfrak{z} > \mathfrak{o}_1$, und da aus $\alpha\chi \equiv \alpha$, $\beta\chi \equiv \beta$ (mod. $\mathfrak{p}^{r+1}$) auch $(\alpha\beta)\chi = \alpha\chi \cdot \beta\chi \equiv \alpha\beta$ (mod. $\mathfrak{p}^{r+1}$) folgt, so ist auch $\mathfrak{o}_1^2 > \mathfrak{o}_1$, w. z. b. w. (D., S. 505). Da $\mathfrak{p}^{r+1} > \mathfrak{o}_1$, so ist der Führer

$$\frac{\mathfrak{o}_1}{\mathfrak{o}} = \mathfrak{p}^k, \quad 0 < k \leqq r+1, \quad (\mathfrak{o}, \mathfrak{o}_1)(\mathfrak{o}_1, \mathfrak{p}^k) = (\mathfrak{o}, \mathfrak{p}^k) = p^{kf},$$
$$0 < h \leqq kf$$

oder vielmehr $0 < h < kf$, weil $\mathfrak{o}_1$ notwendig ein echter Teiler von $\mathfrak{p}^k$ ist.

Nun sei ϱ eine bestimmte durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare Zahl, so ist $\mathfrak{o}\varrho + \mathfrak{p}^2 = \mathfrak{p}$, also $\mathfrak{o}\varrho^r + \mathfrak{p}^{2r} = \mathfrak{o}\varrho^r + \mathfrak{p}^{r+1} = \mathfrak{p}^r$; da nun alle $\omega\chi - \omega$ in $\mathfrak{p}^r$ enthalten sind, so kann man setzen

$$\omega\chi \equiv \omega + \varrho^r d\omega \pmod{\mathfrak{p}^{2r}},$$

wo $d\omega$ eine zu ω gehörige Zahl ist, die mod. $\mathfrak{p}^r$ bestimmt ist. Für alle in $\mathfrak{o}_1$ enthaltenen Zahlen ω_1, und nur für diese, ist

$$d\omega_1 \equiv 0 \pmod{\mathfrak{p}}.$$

Nun folgen aus $(\alpha \pm \beta)\chi = \alpha\chi \pm \beta\chi$ und $(\alpha\beta)\chi = (\alpha\chi)(\beta\chi)$, und aus

$$\alpha\chi \equiv \alpha + \varrho^r d\alpha, \quad \beta\chi \equiv \beta + \varrho^r d\beta \pmod{\mathfrak{p}^{2r}}$$

die Gesetze (Differentialrechnung)

$$d(\alpha \pm \beta) \equiv d\alpha \pm d\beta, \quad d(\alpha\beta) \equiv \beta d\alpha + \alpha d\beta \pmod{\mathfrak{p}^r}$$

und hieraus weiter

$$d(\omega^m) \equiv m\omega^{m-1} d\omega \pmod{\mathfrak{p}^r}.$$

Da hieraus $d(\varrho^2) \equiv 2\varrho d\varrho$ (mod. $\mathfrak{p}^r$), also $d(\varrho^2) \equiv 0$ (mod. $\mathfrak{p}$) folgt, so ist ϱ^2 in $\mathfrak{o}_1$ enthalten; da ferner $\mathfrak{p}^2 = \mathfrak{o}\varrho^2 + \mathfrak{p}^{r+1}$, also jede in $\mathfrak{p}^2$ enthaltene Zahl

$$\pi_2 = \omega\varrho^2 + \pi_{r+1}$$

gesetzt werden kann, wo ω in $\mathfrak{o}$, π_{r+1} in $\mathfrak{p}^{r+1}$ enthalten ist, so folgt $d\pi_2 \equiv \omega d(\varrho^2) + \varrho^2 d\omega + d\pi_{r+1}$ (mod. $\mathfrak{p}^r$), also $d\pi_2 \equiv 0$ (mod. $\mathfrak{p}$), folglich $\mathfrak{p}^2 > \mathfrak{o}_1$, also $k = 1$ oder $= 2$.

[Dieser Satz über die Substitutionen der höheren Verzweigungsgruppen — der, nach der Überschrift zu schließen, vor der Publikation in den Göttinger Nachrichten zu liegen scheint — wurde in der Literatur nie in dieser Fassung ausgesprochen. E. N.]