welches sich bei der Permutation q nur um einen durch x^p-1 teilbaren Bestandteil ändert. Da der Rest von P in Bezug auf den Teiler x^p-1 ganze zyklische Funktionen von $x_0, x_1, \ldots$ zu Koeffizienten hat, so kann

$$P \equiv y_0 g_0(x) + y_1 g_1(x) + \ldots + y_{t-1} g_{t-1}(x) \pmod{x^p-1}$$

gesetzt werden, wo $\Delta^2 g_0, \Delta^2 g_1, \ldots$ ganze Funktionen von $x, x_0, x_1, \ldots$ sind und die Permutationen von Γ vertragen.

Führt man die Permutation r aus und ersetzt zugleich x durch x^a, wodurch alle Ausdrücke $L(x^k)$, $L_1(x^k)$ und daher auch P nach dem Modul x^p-1 ungeändert bleiben, so ergibt sich

$$P \equiv y_1 g_0(x^a) + y_2 g_1(x^a) + \ldots + y_0 g_{t-1}(x^a) \pmod{x^p-1}.$$

Hieraus folgt

$$y_0(g_{t-1}(x^a) - g_0(x)) + y_1(g_0(x^a) - g_1(x)) + \ldots \equiv 0 \pmod{x^p-1}$$

und nach wiederholter Ausführung der Permutation r

$$\begin{gathered} y_1(g_{t-1}(x^a) - g_0(x)) + y_2(g_0(x^a) - g_1(x)) + \ldots \equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ y_{t-1}(g_{t-1}(x^a) - g_0(x)) + y_0(g_0(x^a) - g_1(x)) + \ldots \equiv 0 \\ \pmod{x^p-1}. \end{gathered}$$

Es muß daher

$$\begin{aligned} &g_0(x^a) - g_1(x) \equiv 0 \quad g_1(x) \equiv g_0(x^a) \qquad \pmod{x^p-1} \\ &g_1(x^a) - g_2(x) \equiv 0 \quad g_2(x) \equiv g_1(x^a) \equiv g_0(x^{a^2}) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

sein. Somit ist

$$P \equiv y_0 g_0(x) + y_1 g_0(x^a) + \ldots + y_{t-1} g_0(x^{a^{t-1}}) \pmod{x^p-1}.$$

Denkt man sich nun unter $x_0, x_1, \ldots$ die Wurzeln der gesuchten Gleichung und setzt $x = \alpha^m$, so folgt

$$P(\alpha^m) = y_0 g_0(\alpha^m) + y_1 g_0(\alpha^{ma}) + \ldots + y_{t-1} g_0(\alpha^{ma^{t-1}}),$$

wo jetzt $g_0(x)$ eine ganze Funktion von x mit Koeffizienten in R ist.