Riv. Mat. Univ. Parma (4) **14*** (1988), 69-89

ANDREI DUMA (*)

Automorfismi di corpi di funzioni algebriche

Notazioni

Siano $p \in \boldsymbol{N}$ primo, $m \in \boldsymbol{N}$ e $\boldsymbol{F}_{p^m}$ il corpo con p^m elementi. $PGL(2,\ p^m)$ è il *gruppo lineare proiettivo*, cioè il gruppo delle trasformazioni $\lambda \mapsto \dfrac{a\lambda + b}{c\lambda + d}$ con $a,\ b,\ c,\ d \in \boldsymbol{F}_{p^m}$ e $ad - bc \neq 0$. $PSL(2,\ p^m)$ è il *gruppo lineare proiettivo speciale*, cioè il sottogruppo di $PGL(2,\ p^m)$ che contiene tutte le trasformazioni $\lambda \mapsto \dfrac{a\lambda + b}{c\lambda + d}$ tale che $ad - bc = q^2$ con $q \in \boldsymbol{F}_{p^m}^*$ dove $\boldsymbol{F}_{p^m}^* = \boldsymbol{F}_{p^m} \setminus \{0\}$. Il gruppo delle 2×2-matrici $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con $a,\ b,\ c,\ d \in \boldsymbol{F}_{p^m}$ e $ad - bc = 1$ è il *gruppo lineare speciale*; e si denota con $SL(2,\ p^m)$.

Siano A un gruppo moltiplicativo e B un gruppo additivo, tale che A opera su B. Il *prodotto semidiretto* $A \times_s B$ è l'insieme delle coppie $(a,\ b)$, $a \in A$, $b \in B$ con la legge di moltiplicazione

$$(a_1,\ b_1)(a_2,\ b_2) = (a_1 a_2,\ a_1 b_2 + b_1)\,.$$

1 - Caso classico

Sia X una *superficie di Riemann compatta*, ossia una varietà complessa di dimensione uno connessa e compatta e sia g_X il suo genere. X è quindi omeomorfa ad una sfera con g_X manici od anche, equivalentemente, la dimensione dello

(*) Indirizzo: Fachbereich Mathematik, Fern Universität, Hagen, Bundesrepublik Deutschland.

spazio vettoriale delle forme olomorfe di ordine uno su X è g_X. Sia $\mathscr{F}(X) = \mathrm{Mer}(X)$ il *corpo delle funzioni meromorfe* su X. Questo corpo caratterizza completamente la superficie di Riemann X, poiché si può dimostrare che due *superficie di Riemann compatte sono isomorfe se, e solo se, i corpi delle funzioni meromorfe sono tra loro isomorfi.*

$\mathscr{F}(X)$ ha una struttura algebrica abbastanza semplice come risulta dalla seguente asserzione. Sia f una funzione meromorfa non-costante su X; in generale esiste, per ogni $z \in \boldsymbol{C} \cup \{\infty\}$, lo stesso numero n di punti $P_1, \ldots, P_n \in X$ tali che $f(P_1) = \ldots = f(P_n) = z$. Esiste inoltre una funzione meromorfa h (che dipende da f) su X, tale che

(i) h soddisfa un'equazione $P_h(h) = 0$, dove P_h è un polinomio di grado n con coefficienti razionali, cioè $P_h \in \boldsymbol{C}(f)$

(ii) ogni $l \in \mathscr{F}(X)$ si può rappresentare con un polinomio irriducibile di grado minore o uguale a $n-1$ nella variabile h e i suoi coefficienti sono funzioni razionali di f, cioè

$$l = a_0 + a_1 h + \ldots + a_{n-1} h^{n-1} \qquad a_0, a_1, \ldots, a_{n-1} \in \boldsymbol{C}(f).$$

In conclusione, *il corpo* $\mathscr{F}(X) = \mathrm{Mer}(X)$ *è un'estensione algebrica di grado* n *dell'estensione puramente trascendente* $\boldsymbol{C}(f)$ di $\boldsymbol{C}$; *risulta* $\boldsymbol{C}(f, g) = \mathscr{F}(X)$.

Se esiste $f \in \mathscr{F}(X)$ tale che $\boldsymbol{C}(f) = \mathscr{F}(X)$, allora si dice che $\mathscr{F}(X)$ è *razionale.* In questo caso X è isomorfo a $\boldsymbol{C} \cup \{\infty\}$ o equivalentemente a $\boldsymbol{P}^1(\boldsymbol{C})$. La funzione identità z di $\boldsymbol{C} \cup \{\infty\}$ è una funzione f del tipo precedente.

Il polinomio P_h si può scrivere nella forma $\frac{P}{F}$ dove $P \in \boldsymbol{C}[f, T]$ è irriducibile e $F \in \boldsymbol{C}[f]$. L'equazione $P(x_1, x_2) = 0$ dicesi una *equazione della superficie* X. $\mathscr{F}(X)$ è $\boldsymbol{C}$*-isomorfo a* $\mathrm{Quot}(\boldsymbol{C}[x_1, x_2]/(P))$. Viceversa, *ad ogni polinomio irriducibile* $P \in \boldsymbol{C}[x_1, x_2]$ *corrisponde una superficie di Riemann compatta* X_P *con* $\mathscr{F}(X_P) \approx \mathrm{Quot}(\boldsymbol{C}[x_1, x_2]/(P))$.

Un *automorfismo* della superficie di Riemann X è un'applicazione biolomorfa di X su X. Il gruppo di automorfismi di X si denota con $\mathrm{Aut}(X)$. Ad ogni automorfismo di X corrisponde un automorfismo del corpo $\mathscr{F}(X)$, che lascia $\boldsymbol{C}$ invariante, e viceversa; di conseguenza si ha un isomorfismo di gruppi $\mathrm{Aut}(X) \approx \mathrm{Aut}(\mathscr{F}(X)/\boldsymbol{C})$. Quindi, *lo studio degli automorfismi di* X *è equivalente allo studio degli automorfismi del corpo* $\mathscr{F}(X)$.

Se $g_X = 0$, X è isomorfo a $\boldsymbol{C} \cup \{\infty\}$ e quindi a $\boldsymbol{P}^1(\boldsymbol{C})$; dunque $\mathrm{Aut}(X) \approx \mathrm{Aut}(\boldsymbol{P}^1(\boldsymbol{C})) \approx PGL(2, \boldsymbol{C})$. Pertanto $\mathrm{Aut}(X)$ è un gruppo infinito (preci-

samente una varietà complessa di dimensione tre). È utile scrivere anche $\mathrm{Aut}(X) \approx \mathrm{Aut}(\boldsymbol{C}(z)/\boldsymbol{C}) = \mathrm{Aut}(\boldsymbol{P}^1(\boldsymbol{C}))$.

Se $g_X = 1$, X è isomorfo ad un toro e dunque $\mathrm{Aut}(X)$ è ancora un gruppo infinito. Sia $X \approx \boldsymbol{C}/\boldsymbol{Z}\omega_1 \oplus \boldsymbol{Z}\omega_2$, dove $\omega_1,\ \omega_2 \in \boldsymbol{C}^*$ e $\dfrac{\omega_1}{\omega_2} \notin \boldsymbol{R}$. Allora

$$\mathrm{Aut}(X) \approx \mathrm{Aut}(\boldsymbol{C}/\boldsymbol{Z}\omega_1 \oplus \boldsymbol{Z}\omega_2) = \{\gamma_{t_1,t_2};\ \gamma_{t_1,t_2}([z]) = [z + t_1\omega_1 + t_2\omega_2],\ (t_1,\ t_2) \in [0,\ 1)^2\}$$

dove $[z]$ indica la classe di z in $\boldsymbol{C}/\boldsymbol{Z}\omega_1 \oplus \boldsymbol{Z}\omega_2$.

H. A. Schwarz (1875) ha dimostrato che, *se* $g_X \geq 2$ *il gruppo degli automorfismi di* X *è finito*. A. Hurwitz (1893) ha completato il risultato di Schwarz dimostrando che *il numero* $\mathrm{aut}(X)$ *degli automorfismi di* X *è minore o uguale a* $84(g_X - 1)$. Soltanto nel 1974, L. Greenberg ha dimostrato che *ogni gruppo finito è isomorfo al gruppo* $\mathrm{Aut}(X)$ *di una opportuna superficie di Riemann compatta* X *(con* $g_X \geq 2$*).*

Per lo studio degli automorfismi di una superficie di Riemann compatta è importante conoscere un risultato di F. Klein che afferma che *ogni sottogruppo finito di* $PGL(2,\ \boldsymbol{C})$ *è isomorfo ad un gruppo ciclico* $\mathcal{C}_n = \boldsymbol{Z}/n\boldsymbol{Z}$*, o ad un gruppo diedrale* $\mathcal{D}_n$ *con* $2n$ *elementi, o ad* $\mathcal{A}_4$ *(gruppo delle permutazioni pari di* 4 *elementi o gruppo tetraedrale), o ad* $\mathcal{S}_4$ *(gruppo delle permutazioni su* 4 *elementi o gruppo ottaedrale), o infine, ad* $\mathcal{A}_5$ *(gruppo delle permutazioni pari di* 5 *elementi o gruppo icosaedrale).*

Una presentazione dettagliata dei diversi problemi sugli automorfismi delle superficie di Riemann compatte si trova nel lavoro [5] del 1985.

2 - Caso astratto

Sia $\mathscr{K}$ un corpo algebricamente chiuso di caratteristica $p \geq 0$. Un corpo $\mathscr{F}$ che contiene $\mathscr{K}$ si chiama *corpo di funzioni algebriche* sopra $\mathscr{K}$ se esiste un sottocorpo $\mathscr{F}_0$ di $\mathscr{F}$ tale che $\mathscr{F}_0 = \mathscr{K}(x)$, dove $x \in \mathscr{F}$ è trascendente sopra $\mathscr{K}$, e $\mathscr{F}_0 \subset \mathscr{F}$ è un'estensione algebrica finita. Per il teorema dell'elemento primitivo esistono un polinomio irriducibile $P = T^n + a_1 T^{n-1} + \ldots + a_n \in \mathscr{F}_0[T]$ ed un elemento $y \in \mathscr{F}$, tale che $y^n + a_1 y^{n-1} + \ldots + a_n = 0$ e $\mathscr{F} = \mathscr{K}(x,\ y)$. $\mathscr{F}$ non determina univocamente $\mathscr{F}_0$, x e y.

Il corpo di funzioni algebriche $\mathscr{F}$ si dice *razionale*, se si può trovare $x \in \mathscr{F}$, tale che $\mathscr{F} = \mathscr{K}(x)$. $\mathscr{F}_0$ è dunque un tale corpo. In una maniera un po' più complicata si può definire il genere $g_{\mathscr{F}}$ di $\mathscr{F}$ [4]. Come nel caso classico si ha $g_{\mathscr{F}} = 0$, *se e solo se* $\mathscr{F}$ *è razionale.*

Se la caratteristica p di $\mathscr{K}$ è zero, il gruppo degli automorfismi $\mathrm{Aut}(\mathscr{F}/\mathscr{K})$ è finito per $g_{\mathscr{F}} \geq 2$; il numero $\mathrm{aut}(\mathscr{F}/\mathscr{K})$ degli automorfismi di X è, in questo caso, minore o uguale ad $84(g_X - 1)$. Le dimostrazioni date da Schwarz e da Hurwitz sono ancora valide per $p = 0$ e $g_{\mathscr{F}} \geq 2$.

H. L. Schmid ha dimostrato nel 1938 che anche *per* $p > 0$ *si ha* $\mathrm{aut}(\mathscr{F}/\mathscr{K}) < +\infty$, *se* $g_{\mathscr{F}} \geq 2$. P. Roquette ha dimostrato nel 1970 la *relazione*

$$\mathrm{aut}(\mathscr{F}/\mathscr{K}) \leq 84(g_{\mathscr{F}} - 1)$$

se $p > g_{\mathscr{F}} + 1$ e $g_{\mathscr{F}} \geq 2$ con l'unico caso di eccezione: $p \geq 5$, $\mathscr{F}$ ammette una presentazione del tipo $\mathscr{K}(x, y)$, dove $y^2 = x^p - x$ [17]. In questo caso $g_{\mathscr{F}} = \frac{1}{2}(p-1)$, $\mathrm{aut}(\mathscr{F}/\mathscr{K}) = 8g(g+1)(2g+1)$ ed esiste una successione esatta di gruppi: $0 \to \mathscr{C}_2 \to \mathrm{Aut}(\mathscr{F}/\mathscr{K}) \to PGL(2, p) \to 1$. Anche nel caso $p = g_{\mathscr{F}} + 1$ è valida la valutazione di Hurwitz, ma con un'eccezione [22]: $\mathscr{F} = \mathscr{K}(x, y)$ con $y^p - y = x^3$; in questo caso

$$\mathrm{aut}(\mathscr{F}/\mathscr{K}) = \begin{cases} 3g(g+1) & \text{se } p \equiv 1 \pmod 3 \\ 3g(g+1)(g+2) & \text{se } p \equiv 2 \pmod 3. \end{cases}$$

D. J. Madden e R. C. Valentini hanno dimostrato nel 1983 che *per ogni corpo algebricamente chiuso* $\mathscr{K}$ *di caratteristica* $p > 0$ *e ogni gruppo finito* G *esiste un corpo di funzioni algebriche* $\mathscr{F}$ *sopra* $\mathscr{K}$ *tale che* G *è isomorfo ad* $\mathrm{Aut}(\mathscr{F}/\mathscr{K})$ [14]. Un'altra dimostrazione di questo teorema è stata data nel 1984 da H. Stichtenoth [23].

Per lo sviluppo della teoria è importante stabilire un risultato analogo a quello di F. Klein. Siano $\mathscr{K}$ un corpo algebricamente chiuso di caratteristica $p \geq 0$ e $\mathscr{F}_0$ un corpo razionale sopra $\mathscr{K}$. L. K. Dickson (ved. [13]) ha dimostrato che *ogni sottogruppo finito* $\mathscr{K}$ *di* $\mathrm{Aut}(\mathscr{F}_0/\mathscr{K})$ *è isomorfo a uno di questi gruppi*:

1. $\mathscr{C}_n$ *gruppo ciclico ad* n *elementi*
2. $\mathscr{D}_n$ *gruppo diedrale a* $2n$ *elementi*
3. $\mathscr{A}_4$ *gruppo tetraedrale a* 12 *elementi*
4. $\mathscr{S}_4$ *gruppo ottaedrale a* 24 *elementi*
5. $\mathscr{A}_5$ *gruppo icosaedrale a* 60 *elementi*
6. $\mathscr{E}_p(m)$ *p-gruppo abeliano elementare a* p^m *elementi*

7. $\mathcal{E}_{p(m)} \times_s \mathcal{C}_n$ *prodotto semidiretto di un p-gruppo abeliano elementare che contiene* p^m *elementi per il gruppo ciclico* $\mathcal{C}_n$ *con* $(n, p) = 1$ *e* $n | p^m - 1$

8. $PSL(2, p^m)$

9. $PGL(2, p^m)$.

I casi 6, 7, 8 e 9 possono presentarsi soltanto se $p > 0$.

Il sottogruppo finito $\mathcal{H}$ di $\mathrm{Aut}(\mathcal{F}_0/\mathcal{K})$ determina una partizione dello spazio proiettivo $\boldsymbol{P}_{\mathcal{K}}$ in orbite. Si può trovare un elemento $x \in \mathcal{F}_0$ con $\mathcal{F}_0 = \mathcal{K}(x)$ tale che i generatori di $\mathcal{H}$ e le orbite di $\boldsymbol{P}_{\mathcal{K}}$ rispetto ad $\mathcal{H}$ abbiano una forma semplice. R. Brandt ha dimostrato nella sua tesi il seguente risultato, necessario per le considerazioni ulteriori: *In ognuno dei casi* 1, 2, ..., 9 *si può trovare per* $\mathcal{H}$ *un elemento* $x \in \mathcal{F}_0$ *con* $\mathcal{F}_0 = \mathcal{K}(x)$ *tale che*

1. $\mathcal{C}_n \approx \mathcal{H} = \langle \sigma_n \rangle$ con $\sigma_n(x) = \xi_n x$, dove ξ_n è una radice primitiva di ordine n di 1.

$$\boldsymbol{P}_{\mathcal{K}} = \mathcal{B}_\infty \cup \mathcal{B}_0 \cup \left(\bigcup_{a \in \mathcal{K}^*} \mathcal{B}_a \right) \qquad \text{dove}$$

$\mathcal{B}_\infty = \{P_\infty\}$, P_∞ è il polo di x, $\mathcal{B}_0 = \{P_0\}$, P_0 è lo zero di x,
$\mathcal{B}_a = \{P \in \boldsymbol{P}_{\mathcal{K}};\ P \text{ è uno zero di } x^n - a\}$.

2a. Se $p = 2$ si ha $\mathcal{D}_n \approx \mathcal{H} = \langle \sigma_n, \tau \rangle$, dove $\tau(x) = \dfrac{1}{x}$.

$$\boldsymbol{P}_{\mathcal{K}} = \mathcal{B}_\infty \cup \mathcal{B}_0 \cup \left(\bigcup_{a \in \mathcal{K}^*} \mathcal{B}_a \right) \qquad \text{dove}$$

$\mathcal{B}_\infty = \{P_0, P_\infty\}$, $\mathcal{B}_0 = \{P \in \boldsymbol{P}_{\mathcal{K}};\ P \text{ uno zero di } x^n + 1\}$
$\mathcal{B}_a = \{P \in \boldsymbol{P}_{\mathcal{K}};\ P \text{ uno zero di } x^{2n} - ax^n + 1\}$.

2b. Se $p \neq 2$ e $(n, p) = 1$ si ha $\mathcal{D}_n \approx \mathcal{H} = \langle \sigma_n, \tau \rangle$.

$$\boldsymbol{P}_{\mathcal{K}} = \mathcal{B}_\infty \cup \mathcal{B}^+ \cup \mathcal{B}^- \cup \left(\bigcup_{a \in \mathcal{K} \setminus \{\pm 2\}} \mathcal{B}_a \right) \qquad \text{dove}$$

$\mathcal{B}_\infty = \{P_0, P_\infty\}$
$\mathcal{B}^+ = \{P \in \boldsymbol{P}_{\mathcal{K}};\ P \text{ uno zero di } x^n - 1\}$, $\mathcal{B}^- = \{P \in \boldsymbol{P}_{\mathcal{K}};\ P \text{ uno zero di } x^n + 1\}$
$\mathcal{B}_a = \{P \in \boldsymbol{P}_{\mathcal{K}};\ P \text{ uno zero di } x^{2n} - ax^n + 1\}$.

2c. Se $p \neq 2$ e $n = p$ si ha $\mathscr{D}_n \approx \mathscr{K} = \langle s,\ t \rangle$ con $s(x) = x + 1,\ t(x) = -x$

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_\infty \cup \mathscr{B}_0 \cup \left(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_\infty = \{P_\infty\},\ \mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } x^p - x\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } (x^p - x)^2 - a\}.$

3a. $p \neq 2,\ 3,\ \mathscr{A}_4 \approx \mathscr{K} = \langle t,\ \mu \rangle$ con $\mu(x) = i\dfrac{x+1}{x-1}.$

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_1 \cup \mathscr{B}_2 \cup \left(\bigcup_{a \in \mathscr{K} \setminus \{\pm 2, \pm 2i\sqrt{3}\}} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ polo o zero di } x^5 - x\}$
$\mathscr{B}_1 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } x^4 - 2i\sqrt{3}\,x^2 + 1\}$
$\mathscr{B}_2 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } x^4 + 2i\sqrt{3}\,x^2 + 1\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } \prod_{j=1}^{3} (x^4 - a_j x^2 + 1)\}$
dove $a_1 \in \mathscr{K} \setminus \{\pm 2,\ \pm 2i\sqrt{3}\},\ a_2 = \dfrac{2a_1 + 12}{2 - a_1},\ a_3 = \dfrac{2a_1 - 12}{2 + a_1}.$

3b. $p = 2,\ \mathscr{A}_4 \approx \mathscr{K} = \langle \sigma_3,\ s \rangle.$

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_\infty \cup \mathscr{B}_0 \cup \left(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_\infty = \{P_\infty\}$
$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } x^4 + x\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } (x^4 + x)^3 + a\}.$

3c. $p = 3,\ \mathscr{A}_4 \approx \mathscr{K} = \langle -\tau,\ s \rangle.$

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_\infty \cup \mathscr{B}_0 \cup \left(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_\infty = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ polo o zero di } x^3 - x\}$
$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } x^6 + x^4 + x^2 + 1\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } (x^6 + x^4 + x^2 + 1)^2 - a(x^3 - x)^3\}.$

4a. $p \neq 2,\ 3,\quad \mathscr{S}_4 \approx \mathscr{K} = \langle \sigma_4,\ \mu \rangle.$

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_1 \cup \mathscr{B}_2 \cup \left(\bigcup_{a \in \mathscr{K}^* \setminus \{108\}} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ zero o polo di $x^5 - x\}$
$\mathscr{B}_1 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $x^8 + 14x^4 + 1\}$
$\mathscr{B}_2 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $(x^4+1)(x^8 - 34x^4 + 1)\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $(x^8 + 14x^4 + 1)^3 - a(x^5 - x)^4\}$.

4b. $p = 3$, $\mathscr{S}_4 \approx \mathscr{H} = \langle t,\ s,\ \tau \rangle$.

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_1 \cup \Big(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a\Big) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ polo o zero di $x^3 - x\}$
$\mathscr{B}_1 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $x^6 + x^4 + x^2 + 1\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $(x^6 + x^4 + x^2 + 1)^4 - a(x^3 - x)^6\}$.

5a. $p \neq 2, 3, 5$, $\mathscr{A}_5 \approx \mathscr{H} = \langle \sigma_5,\ \delta \rangle$, dove $\delta(x) = -\dfrac{x+b}{bx+1}$ con $b = -i(\xi_5 + \xi_5^{-1})$.

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_\infty \cup \mathscr{B}_0^* \cup \Big(\bigcup_{a \in \mathscr{K}^* \setminus \{1728i\}} \mathscr{B}_a\Big) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $f_0(x) = x^{20} - 228ix^{15} - 228ix^{15} - 494x^{10} - 228ix^5 + 1\}$
$\mathscr{B}_\infty = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ zero o polo di $f_\infty(x) = x(x^{10} + 11ix^5 + 1)\}$
$\mathscr{B}_0^* = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $f_0^*(x) = x^{30} + 522i(x^{25} - x^5) + 10.005(x^{20} - x^{10}) - 1\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $(f_0(x))^3 - a(f_\infty(x))^5\}$.

5b. $p = 3$, $\mathscr{A}_5 \approx \mathscr{H} = \langle \sigma_5,\ -\delta \rangle$.

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_\infty \cup \Big(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a\Big) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $g_0(x) = x^{10} - 1\}$
$\mathscr{B}_\infty = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ polo o zero $g_\infty(x) = x(x^{10} + 2ix^5 + 1)\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $(g_0(x))^6 - a(g_\infty(x))^5\}$.

5c. $p = 5$, $\mathscr{A}_5 \approx \mathscr{H} = \langle t,\ s,\ -\tau \rangle$.

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_\infty \cup \Big(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a\Big) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $h_0(x) = (x^5 - x)^4 + 1\}$
$\mathscr{B}_\infty = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ polo o zero di $h_\infty(x) = x^5 - x\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P$ uno zero di $(h_0(x))^3 - a(h_1(x))^{10}\}$.

5d. $p=2$, $\mathscr{A}_5 \approx \mathscr{K} = \langle \sigma_3,\ s,\ \tau \rangle$.

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_\infty \cup \left(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } k_0(x) = (x^4 + x)^3 + 1\}$
$\mathscr{B}_\infty = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ polo o zero di } k_\infty(x) = x^4 + x\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } (k_0(x))^5 + a(k_\infty(x))^{12}\}$.

6. $\mathscr{E}_p(m) \approx \mathscr{T} = \{\tau_b;\ \tau_b(x) = x + b,\ b \in \mathscr{U}\}$, dove $\mathscr{U}$ è un sottogruppo del gruppo additivo $(\mathscr{K}, +)$ di ordine p^m.

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_\infty \cup \left(\bigcup_{a \in \mathscr{K}} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_\infty = \{P_\infty\}$, $\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } \prod_{b \in \mathscr{U}} (x + b) - a\}$.

7. $\mathscr{E}_p(m) \times_s \mathscr{C}_n \approx \mathscr{H} = \langle \sigma_n,\ \tau \rangle$ con np^m elementi e $n | p^m - 1$. Siano $t \in \boldsymbol{N}$ con $nt = p^m - 1$ e $b_1, \ldots, b_t \in \mathscr{K}$ tali che $\mathscr{U} = \{b \in \mathscr{K};\ b \text{ uno zero di } x \prod_{j=1}^{t} (x^n - b_j)\}$. $\mathscr{U}$ è invariante per le rotazioni di periodo n attorno o, cioè $\xi_n\, \mathscr{U} = \mathscr{U}$. Allora

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_\infty \cup \left(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } x \prod_{j=1}^{t} (x^n - b_j) = d_0(x)\}$
$\mathscr{B}_\infty = \{P_\infty\}$, $\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } (d_0(x))^n - a\}$.

8a. $p \neq 2$, $PSL(2,\ p^m) \approx \mathscr{H} = \langle (\sigma_{p^m-1})^2,\ s,\ -\tau \rangle$.

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_\infty \cup \left(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } l_0(x) = (x^n - x)^{n-1} + 1\}$
$\mathscr{B}_\infty = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ polo o zero di } l_\infty(x) = x^n - x\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } (l_0(x))^{(n+1)/2} - a(l_\infty(x))^{(n(n-1))/2}\}$ ed $n = p^m$.

8b. $p = 2$ e 9.
Poiché la funzione $\boldsymbol{F}_{2^m} \to \boldsymbol{F}_{2^m}$, $\lambda \mapsto \lambda^2$ è biiettiva, $PSL(2,\ 2^m) = PGL(2,\ 2^m)$. Quindi i casi 8b e 9 si possono considerare insieme. $\mathscr{H} = \langle \sigma_{p^m-1},\ s,\ \tau \rangle$.

$$\boldsymbol{P}_{\mathscr{K}} = \mathscr{B}_0 \cup \mathscr{B}_\infty \cup \left(\bigcup_{a \in \mathscr{K}^*} \mathscr{B}_a \right) \qquad \text{dove}$$

$\mathscr{B}_0 = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } l_0(x)\}$
$\mathscr{B}_\infty = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ polo o zero di } l_\infty(x)\}$
$\mathscr{B}_a = \{P \in \boldsymbol{P}_{\mathscr{K}};\ P \text{ uno zero di } (l_0(x))^{n+1} - a(l_\infty(x))^{n(n-1)}\}$.

Siano $\mathscr{K}$ un corpo algebricamente chiuso di caratteristica $p \geq 0$, $\mathscr{F}_0 \supset \mathscr{K}$ un'estensione trascendente di ordine uno, $\mathscr{F} \supset \mathscr{F}_0$ un'estensione algebrica di ordine n. In altri termini $\mathscr{F}$ è un corpo di funzioni algebriche sopra $\mathscr{K}$.

Un automorfismo $\sigma \in \mathrm{Aut}(\mathscr{F}_0/\mathscr{K})$ si dice *prolungabile a* $\mathscr{F}$, se esiste un automorfismo $\sigma' \in \mathrm{Aut}(\mathscr{F}/\mathscr{K})$ tale che il diagramma

$$\begin{array}{ccc} \mathscr{F}_0 & \hookrightarrow & \mathscr{F} \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma'} \\ \mathscr{F}_0 & \hookrightarrow & \mathscr{F} \end{array}$$

risulti commutativo. Si dice che σ' è un *prolungamento di* σ.

Sia $\mathscr{G}_0 \subset \mathrm{Aut}(\mathscr{F}_0/\mathscr{K})$ un sottogruppo finito. $\mathscr{G}_0$ si dice *prolungabile a* $\mathscr{F}$, se ogni $\sigma \in \mathscr{G}_0$ ha esattamente n prolungamenti a $\mathscr{F}$.

Sia $\mathscr{G}$ l'insieme di tutti i prolungamenti degli elementi di $\mathscr{G}_0$. $\mathscr{G}_0$ si dice *centralmente prolungabile a* $\mathscr{F}$, se $\mathscr{G}_0$ è prolungabile a $\mathscr{F}$, l'insieme $\mathscr{G}$ è un gruppo e il gruppo di Galois di $\mathscr{F}/\mathscr{F}_0$ è contenuto nel centro $Z(\mathscr{G})$ di $\mathscr{G}$.

3 - Estensioni di Kummer. Recenti risultati di R. Brandt

Si consideri la seguente situazione. Sia $\mathscr{F}$ un corpo di funzioni algebriche sul sottocorpo $\mathscr{K}$ di caratteristica p e $g_{\mathscr{F}} \geq 2$ il genere di $\mathscr{F}$. Siano $\mathscr{Z}$, $\mathscr{G}$ due sottogruppi (finiti) di $\mathrm{Aut}(\mathscr{F}/\mathscr{K})$ con $\mathscr{Z} \subset \mathscr{G}$ e $\mathscr{Z} \approx \mathscr{C}_q$ con q primo e $p \neq q$, $\mathscr{Z} \subset Z(\mathscr{G})$. Si pone $\mathscr{F}_0 = \mathrm{Fix}(\mathscr{Z})$ razionale. Dunque $\mathscr{G}/\mathscr{Z}$ è isomorfo ad un sottogruppo $\mathscr{G}_0$ (in generale non commutativo) di $\mathrm{Aut}(\mathscr{F}_0/\mathscr{K})$; di conseguenza $\mathscr{G}_0$ è uno dei nove gruppi determinati da Dickson. Si ha la successione esatta

$$0 \to \mathscr{Z} \to \mathscr{G} \to \mathscr{G}_0 \to 1\,.$$

In questa situazione parliamo di un'*estensione di Kummer* di tipo $[\mathscr{G}_0|q,\ p]$. Nel 1888 Hurwitz ha osservato nel caso $\mathscr{K} = \boldsymbol{C}$ e nel 1934 Hasse ha dimostrato nel caso generale, che esistono $x,\ y \in \mathscr{F}$ tali che $\mathscr{F}_0 = \mathscr{K}(x)$, $\mathscr{F} = \mathscr{K}(x,\ y)$ e $y^q = \prod_{j=1}^{n} (x - a_j)^{k_j}$, $1 \leq k_j \leq q-1$. Quest'equazione di $\mathscr{F}$ è già abbastanza generale.

R. Brandt ha utilizzato la possibilità di scegliere un altro elemento x^* di $\mathscr{F}$ in luogo di x, per il quale $\mathscr{G}_0$ definisce orbite in $\boldsymbol{P}_{\mathscr{K}}$ che sono date da polinomi speciali e in questo modo ha trovato equazioni più precise per $\mathscr{F}$. Per queste considerazioni abbiamo bisogno di sapere *quanti* (a meno di un'equivalenza) e *quali* gruppi finiti $\mathscr{G}$ appaiono in queste successioni esatte

$$0 \to \mathscr{G}_q \to \mathscr{G} \to \mathscr{G}_0 \to 1 .$$

Conviene ora fare una breve digressione nella *teoria delle estensioni di gruppi* ([7], [8], [18], [21]).

Siano $\mathscr{G}$ un gruppo e $\boldsymbol{Z}\mathscr{G}$ l'anello a coefficienti interi sopra $\mathscr{G}$. Un elemento di $\boldsymbol{Z}\mathscr{G}$ è una somma finita $\sum n_j g_j$ con $n_j \in \boldsymbol{Z}$ e $g_j \in \mathscr{G}$. Le operazioni dell'anello sono

$$\sum n_j g_j + \sum m_j g_j = \sum (n_j + m_j) g_j$$

$$(\sum n_j g_j)(\sum m_k g_k) = \sum_{(j,k)} (n_j m_k)(g_j g_k) .$$

Siano $\mathscr{A}$ un gruppo commutativo e $\mathscr{G}$ un gruppo arbitrario. Una successione esatta di gruppi e di omomorfismi di gruppi

$$0 \to \mathscr{A} \xrightarrow{\tau} \mathscr{E} \xrightarrow{\psi} \mathscr{G} \to 1$$

si chiama un'*estensione* di $\mathscr{A}$ mediante $\mathscr{G}$ (un'*estensione centrale* di $\mathscr{A}$ mediante $\mathscr{G}$), se $\mathscr{A}$ è un sottogruppo normale di $\mathscr{E}$ (se $\mathscr{A} \subset Z(\mathscr{E}) =$ centro di $\mathscr{E}$).

Si osservi che ogni estensione di $\mathscr{A}$ mediante $\mathscr{G}$ definisce un omomorfismo $\pi: \mathscr{G} \to \mathrm{Aut}(\mathscr{A})$ e di conseguenza ogni estensione di $\mathscr{A}$ mediante $\mathscr{G}$ definisce su $\mathscr{A}$ una struttura di $\boldsymbol{Z}\mathscr{G}$-*modulo*.

Sia $\mathscr{A}$ uno $\boldsymbol{Z}\mathscr{G}$-modulo; in particolare $\mathscr{A}$ è un gruppo commutativo. Un'estensione del gruppo $\mathscr{A}$ mediante $\mathscr{G}$ si chiama un'*estensione dello* $\boldsymbol{Z}\mathscr{G}$ *modulo* $\mathscr{A}$ mediante $\mathscr{G}$, se la moltiplicazione di elementi di $\mathscr{A}$ per elementi di $\boldsymbol{Z}\mathscr{G}$, definita dalla struttura di $\boldsymbol{Z}\mathscr{G}$-modulo di $\mathscr{A}$, e la moltiplicazione $\boldsymbol{Z}\mathscr{G} \times \mathscr{A} \to \mathscr{A}$, definita utilizzando l'omomorfismo π, coincidono. Uno $\boldsymbol{Z}\mathscr{G}$-modulo si chiama *banale*, se $ga = a$ per ogni $g \in \mathscr{G}$ e $a \in \mathscr{A}$. Per un'estensione $0 \to \mathscr{A} \to \mathscr{E} \to \mathscr{G} \to 1$ dello $\boldsymbol{Z}\mathscr{G}$-modulo mediante il gruppo $\mathscr{G}$ sono equivalenti le seguenti asserzioni:

$\mathscr{A}$ è uno $\boldsymbol{Z}\mathscr{G}$-modulo banale

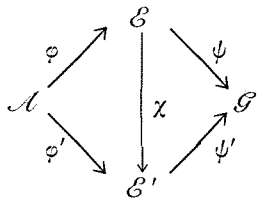
$\mathscr{A}$ è contenuto nel centro di $\mathscr{E}$ (cioè l'estensione data è centrale)

$\pi: \mathcal{G} \to \mathrm{Aut}(\mathcal{A})$ indotta da quest'estensione è banale, cioè $\pi(g) = \mathrm{id}_{\mathcal{A}}$ per ogni $g \in \mathcal{G}$.

Due estensioni

$$0 \to \mathcal{A} \xrightarrow{\varphi} \mathcal{E} \xrightarrow{\psi} \mathcal{G} \to 1, \qquad 0 \to \mathcal{A} \xrightarrow{\varphi'} \mathcal{E}' \xrightarrow{\psi'} \mathcal{G} \to 1$$

si dicono *equivalenti*, se esiste un isomorfismo di gruppi $\chi: \mathcal{E} \to \mathcal{E}'$ tale che il diagramma



sia commutativo.

Sia $\mathrm{e}(\mathcal{G}, \mathcal{A})$ (risp. $\mathrm{E}(\mathcal{G}, \mathcal{A})$) l'insieme delle classi d'equivalenza delle estensioni (risp. delle estensioni centrali) dello $\mathbf{Z}\mathcal{G}$-modulo. $\mathcal{A}$ mediante $\mathcal{G}$. Il numero degli elementi di $\mathrm{e}(\mathcal{G}, \mathcal{A})$ è dunque maggiore o uguale a quello di $\mathrm{E}(\mathcal{G}, \mathcal{A})$. Se $\mathcal{A}$ è uno $\mathbf{Z}\mathcal{G}$-modulo banale, allora il teorema dei coefficienti universali nel caso $n = 2$ dà la possibilità di calcolare $\mathrm{e}(\mathcal{G}, \mathcal{A})$. Precisamente

$$\mathrm{e}(\mathcal{G}, \mathcal{A}) \approx H^2(\mathcal{G}, \mathcal{A}) \approx \mathrm{Hom}_{\mathbf{Z}}(H_2(\mathcal{G}, \mathbf{Z}), \mathcal{A}) \oplus \mathrm{Ext}^1_{\mathbf{Z}}(H_1(\mathcal{G}, \mathbf{Z}), \mathcal{A}).$$

Per $\mathcal{G}_0 \in \{\mathcal{C}_n, \mathcal{D}_n, \ldots, PSL(2, p^m), PGL(2, p^m)\}$, dei gruppi di omologia $H_1(\mathcal{G}_0, \mathbf{Z})$, $H_2(\mathcal{G}_0, \mathbf{Z})$ che appaiono in questa formula alcuni sono ben noti, altri sono stati calcolati da R. Brandt in [1]. $H_1(\mathcal{G}_0, \mathbf{Z})$ è isomorfo a $\mathcal{G}_0/K(\mathcal{G}_0)$, dove $K(\mathcal{G}_0)$ è il *commutatore* di $\mathcal{G}_0$, cioè il più piccolo sottogruppo di $\mathcal{G}_0$ che contiene tutti i prodotti della forma $g_1 g_2 g_1^{-1} g_2^{-2}$ con $g_1, g_2 \in \mathcal{G}_0$ ovvero il più grande sottogruppo normale di $\mathcal{G}_0$. Si ha ([2], [18], [20]):

1. $H_1(\mathcal{C}_n, \mathbf{Z}) \approx \mathcal{C}_n$ $\qquad$ $H_2(\mathcal{C}_n, \mathbf{Z}) = 1$

2. $$H_1(\mathcal{D}_n, \mathbf{Z}) \approx \begin{cases} \mathcal{C}_2 & \text{se } n \equiv 1 \bmod 2 \\ \mathcal{C}_2 \times \mathcal{C}_2 & \text{se } n \equiv 0 \bmod 2 \end{cases}$$

$$H_2(\mathcal{D}_n, \mathbf{Z}) \approx \begin{cases} 1 & \text{se } n \equiv 1 \bmod 2 \\ \mathcal{C}_2 & \text{se } n \equiv 0 \bmod 2 \end{cases}$$

3. $H_1(\mathcal{A}_4, \mathbf{Z}) \approx \mathcal{C}_3$ $\quad H_2(\mathcal{A}_4, \mathbf{Z}) \approx \mathcal{C}_2$

4. $H_1(\mathcal{S}_4, \mathbf{Z}) \approx \mathcal{C}_2$ $\quad H_2(\mathcal{S}_4, \mathbf{Z}) \approx \mathcal{C}_2$

5. $H_1(\mathcal{A}_5, \mathbf{Z}) = 1$ $\quad H_2(\mathcal{A}_5, \mathbf{Z}) \approx \mathcal{C}_2$

6. $H_1(\mathcal{E}_p(m), \mathbf{Z}) = 1$ $\quad H_2(\mathcal{E}_p(m), \mathbf{Z}) \approx (\mathcal{C}_2)^{(p^m-1)!}$

7. $H_1(\mathcal{E}_p(m) \times_s \mathcal{C}_n, \mathbf{Z}) \approx \mathcal{C}_n$ $\quad H_2(\mathcal{E}_p(m) \times_s \mathcal{C}_n, \mathbf{Z})$ è un p-gruppo abeliano elementare

8. $H_1(PSL(2, p^m), \mathbf{Z}) = 1$ se $p^m \neq 2, 3$

$$H_2(PSL(2, p^m), \mathbf{Z}) \approx \begin{cases} \mathcal{C}_2 & \text{se } p > 2 \text{ e } p^m \neq 9 \\ 1 & \text{se } p = 2 \text{ e } p^m \neq 4 \\ \mathcal{C}_2 & \text{se } p^m = 2 \\ \mathcal{C}_6 & \text{se } p^m = 9 \end{cases}$$

9. $H_1(PGL(2, p^m), \mathbf{Z}) \approx \mathcal{C}_2$ se $p \neq 2$

$H_2(PGL(2, p^m), \mathbf{Z}) \approx \mathcal{C}_2$.

Dopo lunghissimi calcoli R. Brandt ha potuto determinare *l'elenco delle classi di isomorfia* $\mathrm{E}(\mathcal{G}_0, \mathcal{C}_q)$ *delle estensioni centrali di* $\mathcal{C}_q$ *mediante il gruppo* $\mathcal{G}_0 \in \{\mathcal{C}_n, \mathcal{D}_n, \ldots, PSL(2, p^m), PGL(2, p^m)\}$ dove q è un numero primo, non necessariamente $p \neq q$. Il risultato è questo:

1. $\mathrm{E}(\mathcal{C}_n, \mathcal{C}_p) = \{\mathcal{C}_p \times \mathcal{C}_n\}$ se $(n, q) = 1$ $\quad \mathrm{E}(\mathcal{C}_q, \mathcal{C}_q) = \{\mathcal{C}_q \times \mathcal{C}_q, \mathcal{C}_{q^2}\}$

2a. $n \equiv 1 \bmod 2$

$$\mathrm{E}(\mathcal{D}_n, \mathcal{C}_q) = \begin{cases} \{\mathcal{C}_q \times \mathcal{D}_n\} & \text{se } q \geq 3 \\ \{\mathcal{C}_2 \times \mathcal{D}_n, \mathcal{G}_n\} & \text{se } q = 2. \end{cases}$$

Coxeter denota con $\langle 2, 2, n \rangle$ il gruppo diciclico $\mathcal{G}_n$ di ordine $4n$ generato da S e T con le relazioni $S^{2n} = 1$, $S^n = T^2$, $T^{-1}ST = S^{-1}$.

2b. $n \equiv 0 \bmod 2$

$$\mathrm{E}(\mathcal{D}_n, \mathcal{C}_q) = \begin{cases} \{\mathcal{C}_q \times \mathcal{D}_n\} & \text{se } q \geq 3 \\ \{\mathcal{C}_2 \times \mathcal{D}_2, \mathcal{D}_4, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{Q}_8\} & \text{se } n = q = 2 \\ \{\mathcal{C}_2 \times \mathcal{D}_n, \mathcal{D}_{2n}, \mathcal{G}_n, \mathcal{K}_n, \mathcal{U}_n, \mathcal{V}_n\} & \text{se } n \neq 2, q = 2. \end{cases}$$

$\mathscr{H}_n = \langle 2, 2|n, 2\rangle$ è il gruppo con generatori R e S e con le relazioni $R^2 = S^2$, $(RS)^n = R^4 = 1$.

$\mathscr{U}_n = \langle n, 2|2, 2\rangle$ è generato da S e T con le relazioni $S^{2n} = T^2 = 1$ e $TST = S^{n-1}$.

$\mathscr{V}_n = \langle 4, n|2, 2\rangle$ è generato da S e T, dove si ha $R^4 = S^n = (RS)^2 = (R^{-1}S)^2 = 1$.

$\mathscr{Q}_8$ è il gruppo dei quaternioni.

3.
$$\mathrm{E}(\mathscr{A}_4,\ \mathscr{C}_q) = \begin{cases} \{\mathscr{C}_q \times \mathscr{A}_4\} & \text{se } q \geqslant 5 \\ \{\mathscr{C}_3 \times \mathscr{A}_4,\ (\mathscr{C}_2 \times \mathscr{C}_2) \times_s \mathscr{C}_9\} & \text{se } q = 3 \\ \{\mathscr{C}_2 \times \mathscr{A}_4,\ SL(2, 3)\} & \text{se } q = 2. \end{cases}$$

4.
$$\mathrm{E}(\mathscr{S}_4,\ \mathscr{C}_q) = \begin{cases} \{\mathscr{C}_q \times \mathscr{S}_4\} & \text{se } q \geqslant 3 \\ \{\mathscr{C}_2 \times \mathscr{S}_4,\ \mathscr{W}_1,\ \mathscr{W}_2,\ \mathscr{W}_3\} & \text{se } q = 2 \end{cases}$$

dove la successione $0 \to \mathscr{C}_2 \to \mathscr{W}_j \to \mathscr{S}_4 \to 1$ è esatta, i gruppi $\mathscr{W}_1$, $\mathscr{W}_2$, $\mathscr{W}_3$, hanno rispettivamente i numeri 48.49, 48.37, 48.50 nel lavoro di Neubüser [15] che contiene tutti i gruppi di ordine $\leqslant 100$ ad eccezione di quelli di ordine 64 e 96.

5.
$$\mathrm{E}(\mathscr{A}_5,\ \mathscr{C}_q) = \begin{cases} \{\mathscr{C}_q \times \mathscr{A}_5\} & \text{se } q \geqslant 3 \\ \{\mathscr{C}_2 \times \mathscr{A}_5,\ SL(2, 5)\} & \text{se } q = 2. \end{cases}$$

6. $\mathrm{E}(\mathscr{E}_p(m),\ \mathscr{C}_q) = \{\mathscr{C}_q \times \mathscr{E}_p(m)\}$ se $(q,\ p) = 1$.

7.
$$\mathrm{E}(\mathscr{E}_p(m) \times_s \mathscr{C}_n,\ \mathscr{C}_q) = \begin{cases} \{\mathscr{C}_q \times (\mathscr{E}_p(m) \times_s \mathscr{C}_n)\} & \text{se } (q,\ n) = 1 \\ \{\mathscr{C}_q \times (\mathscr{E}_p(m) \times_s \mathscr{C}_n),\ \mathscr{E}_p(m) \times_s \mathscr{C}_{qn}\} & \text{se } (q,\ n) = q. \end{cases}$$

8.
$$\mathrm{E}(PSL(2, p^m),\ \mathscr{C}_q) = \begin{cases} \{\mathscr{C}_2 \times PSL(2, 4),\ SL(2, 5)\} & \text{se } q = 2,\ p^m = 4 \\ \{\mathscr{C}_2 \times PSL(2, 2),\ \mathscr{C}_3\} & \text{se } q = 2,\ p^m = 2 \\ \{\mathscr{C}_2 \times PSL(2, p^m),\ SL(2, p^m)\} & \text{se } q = 2,\ p \neq 2 \\ \{\mathscr{C}_3 \times PSL(2, 3),\ (\mathscr{C}_2 \times \mathscr{C}_2) \times_s \mathscr{C}_9\} & \text{se } q = 3,\ p^m = 3 \\ \{\mathscr{C}_q \times PSL(2, p^m)\} & \text{negli altri casi.} \end{cases}$$

9. Se $p \neq 2$ si ha

$$\mathrm{E}(PGL(2, p^m),\ \mathscr{C}_q) = \begin{cases} \{\mathscr{C}_q \times PGL(2, p^m)\} & \text{se } q \neq 2 \\ \{\mathscr{C}_2 \times PGL(2, p^m),\ \mathscr{D}_1(p^m),\ \mathscr{D}_2(p^m),\ \mathscr{D}_3(p^m)\} & \text{se } q = 2. \end{cases}$$

Le definizioni di $\mathscr{D}_1(p^m)$, $\mathscr{D}_2(p^m)$, $\mathscr{D}_3(p^m)$ si trovano nel lavoro [20] (v. anche [1].

Se $p=2$ si ha

$$\mathrm{E}(PGL(2,2^m),\ \mathcal{G}_q)=\begin{cases}\{\mathcal{G}_2\times PGL(2,2^2),\ SL(2,5)\} & \text{se } q=2,\ m=2\\ \{\mathcal{G}_2\times PGL(2,2),\ \mathcal{G}_3\} & \text{se } q=2,\ m=1\\ \{\mathcal{G}_q\times PGL(2,2^m)\} & \text{negli altri casi.}\end{cases}$$

Utilizzando questo risultato R. Brandt ha dimostrato che *per tutte le estensioni di Kummer del tipo* $[\mathcal{G}_0|q,\ p]$, *con* $\mathcal{G}_0\in\{\mathcal{C}_n,\ \mathcal{D}_n,\ \ldots,\ PSL(2,p^m),\ PGL(2,p^m)\}$ *e* $q\neq p$ *numeri primi, sussistono le equazioni seguenti:*

Se $\mathcal{G}_0=\mathcal{C}_n$

$$y^q=x^{k_0}\prod_{j=1}^{m}(x^n-a_j)^{k_j} \tag{1}$$

dove $0\leqslant k_0<q,\quad 1\leqslant k_j<q,\ a_1,\ \ldots,\ a_m\in K^*$ a due a due diversi.

Se $\mathcal{G}_0=\mathcal{D}_n$ con $n>2$, n pari e $(n,\ p)=1,\ q=2$

$$y^2=x^{\nu_0}(x^n-1)^{\nu_1}(x^n+1)^{\nu_2}\prod_{j=1}^{k}(x^{2n}-b_jx^n+1) \tag{2a'}$$

dove $\nu_i\in\{0,\ 1\},\quad b_1,\ \ldots,\ b_k\in\mathcal{K}\setminus\{\pm 2\}$ a due a due diversi.

Se $\mathcal{G}_0=\mathcal{D}_2,\ q=2$

$$y^2=x^{\nu_0}[(x^2-1)(x^2+1)]^{\nu_1}\prod_{j=1}^{k}(x^4-b_jx^2+1) \tag{2a''}$$

dove $\nu_j\in\{0,\ 1\},\ b_1,\ \ldots,\ b_k\in\mathcal{K}\setminus\{\pm 2\}$ a due a due diversi.

Se $\mathcal{G}_0=\mathcal{D}_{2n+1}$ con $(2n+1,\ p)=1,\ q=2$

$$y^2=x^{\nu_0}[(x^n-1)(x^n+1)]^{\nu_1}\prod_{j=1}^{k}(x^{2n}-b_jx^n+1) \tag{2b}$$

dove $\nu_0,\ \nu_1\in\{0,\ 1\},\quad b_1,\ \ldots,\ b_k\in\mathcal{K}\setminus\{\pm 2\}$ a due a due diversi.

Se $\mathcal{G}_0=\mathcal{D}_p,\ q=2$

$$y^2=(x^p-x)^{\nu}\prod_{j=1}^{k}[(x^p-x)^2-b_j] \tag{2c}$$

dove $\nu \in \{0, 1\}$, $b_1, \ldots, b_k \in \mathscr{K}^*$ a due a due diversi.

Se $\mathscr{G}_0 = \mathscr{D}_n$ con $(p, 2n) = 1$, $n \equiv 0 \bmod q$, $q \geq 3$

$$y^q = (x^n - 1)^{\nu_1}(x^n + 1)^{\nu_2} \prod_{j=1}^{m} (x^{2n} - b_j x^n + 1)^{k_j} \tag{2d'}$$

dove $0 \leq \nu_1, \nu_2 < q$, $1 \leq k_j < q$, $b_1, \ldots, b_m \in \mathscr{K} \setminus \{\pm 2\}$ a due a due diversi.

Se $\mathscr{G}_0 = \mathscr{D}_n$ con $(p, 2n) = 1$, $n \not\equiv 0 \bmod q$, $q \geq 3$

$$y^q = x^{\nu_0}(x^n - 1)^{\nu_1}(x^n + 1)^{\nu_2} \prod_{j=1}^{m} (x^{2n} - b_j x^n + 1)^{k_j} \tag{2d''}$$

dove $0 \leq \nu_0, \nu_1, \nu_2 < q$, $1 \leq k_j < q$, $b_1, \ldots, b_m \in \mathscr{K} \setminus \{\pm 2\}$ a due a due diversi, $2\nu_0 + n(\nu_1 + \nu_2) + 2n \sum_{j=1}^{m} k_j \equiv 0 \bmod q$.

Se $\mathscr{G}_0 = \mathscr{D}_p$ con $p \neq 2$, $q \geq 3$

$$y^q = (x^p - x)^{\nu} \prod_{j=1}^{m} [(x^p - x) - b_j]^{k_j} \tag{2e}$$

dove $0 \leq \nu < q$, $1 \leq k_j < q$, $b_1, \ldots, b_m \in \mathscr{K}^*$ a due a due diversi.

Se $\mathscr{G}_0 = \mathscr{D}_n$ con $(n, 2) = 1$, $n \equiv 0 \bmod q$, $q \geq 3$, $p = 2$

$$y^q = (x^n + 1)^{\nu} \prod_{j=1}^{m} (x^{2n} + b_j x^n + 1)^{k_j} \tag{2f'}$$

dove $0 \leq \nu < q$, $1 \leq k_j < q$, $b_1, \ldots, b_m \in \mathscr{K}^*$ a due a due diversi.

Se $\mathscr{G}_0 = \mathscr{D}_n$ con $(n, 2) = 1$, $n \not\equiv 0 \bmod q$, $q \geq 3$, $p = 2$

$$y^q = x^{\nu_0}(x^n + 1)^{\nu_1} \prod_{j=1}^{m} (x^{2n} + b_j x^n + 1)^{k_j} \tag{2f''}$$

dove $0 \leq \nu_0, \nu_1 < q$, $1 \leq k_j < q$, $b_1, \ldots, b_m \in \mathscr{K}^*$ a due a due diversi, $2n + n\nu_1 + 2n \sum_{j=1}^{m} k_j \equiv 0 \bmod q$.

Se $\mathscr{G}_0 = \mathscr{A}_4$, $q = 2$, $p = 3$

$$y^2 = (x^3 - x)^{\nu_0}(x^6 + x^4 + x^2 + 1)^{\nu_1} \prod_{j=1}^{m} [(x^6 + x^4 + x^2 + 1)^2 - a_j(x^3 - x)^3] \tag{3a'}$$

dove $\nu_0, \nu_1 \in \{0, 1\}$, $a_1, \ldots, a_m \in \mathscr{K}^*$ a due a due diversi.

Se $\mathcal{G}_0 = \mathcal{A}_4$, $q = 2$, $p \notin \{2, 3\}$

$$(3a'') \qquad y^2 = (x^5 - x)^{\nu_0}(x^4 - 2i\sqrt{3}\,x^2 + 1)^{\nu_1}(x^4 + 2i\sqrt{3}\,x^2 + 1)^{\nu_2} \prod_{j=1}^{m} [\prod_{k=1}^{3} (x^4 - b_{jk}\,x^2 + 1)]$$

dove $\nu_i \in \{0, 1\}$, $b_{jk} \in \mathcal{K} \setminus \{\pm 2, \pm 2i\sqrt{3}\}$ a due a due diversi,

$$b_{j2} = \frac{2b_{j1} + 12}{2 - b_{j1}} \qquad b_{j3} = \frac{2b_{j1} - 12}{2 + b_{j1}}.$$

Se $\mathcal{G}_0 = \mathcal{A}_4$, $q = 3$, $p = 2$

$$(3b') \qquad y^3 = (x^4 + x)^{\nu} \prod_{j=1}^{m} [(x^4 + x)^3 + a_j]^{k_j}$$

dove $0 \leqslant \nu < 3$, $1 \leqslant k_j < 3$, $a_1, \ldots, a_m \in \mathcal{K}^*$ a due a due diversi.

Se $\mathcal{G}_0 = \mathcal{A}_4$, $q = 3$, $p \notin \{2, 3\}$

$$(3b'') \qquad y^3 = (x^5 - x)^{\nu_0}(x^4 - 2i\sqrt{3}\,x^2 + 1)^{\nu_1}(x^4 + 2i\sqrt{3}\,x^2 + 1)^{\nu_2} \prod_{j=1}^{m} [\prod_{r=1}^{3} (x^4 - b_{jr}x^2 + 1)]^{k_j}$$

dove $0 \leqslant \nu_i < 3$, $k_j \in \{1, 2\}$, $b_{jr} \in \mathcal{K} \setminus \{\pm 2, \pm 2i\sqrt{3}\}$ a due a due diversi

$$b_{j2} = \frac{2b_{j1} + 12}{2 - b_{j1}} \qquad b_{j3} = \frac{2b_{j1} - 12}{2 + b_{j1}} \qquad \nu_1 + \nu_2 \equiv 0 \mod 3.$$

Se $\mathcal{G}_0 = \mathcal{A}_4$, $q \notin \{2, 3\}$, $p = 2$

$$(3c') \qquad y^q = (x^4 + x)^{\nu} \prod_{j=1}^{m} [(x^4 + x)^3 + a_j]^{k_j}$$

dove $0 \leqslant \nu < q$, $1 \leqslant k_j < q$, $a_1, \ldots, a_m \in \mathcal{K}^*$ a due a due diversi.

Se $\mathcal{G}_0 = \mathcal{A}_4$, $q \notin \{2, 3\}$, $p \geqslant 3$

$$(3c'') \qquad y^q = (x^5 - x)^{\nu_0}(x^4 - 2i\sqrt{3}\,x^2 + 1)^{\nu_1}(x^4 + 2i\sqrt{3}\,x^2 + 1)^{\nu_2} \prod_{j=1}^{m} [\prod_{r=1}^{3} (x^4 - b_{jr}x^2 + 1)]^{k_j}$$

dove $0 \leqslant \nu_j < q$, $1 \leqslant k_j < q$, $b_{jr} \in \mathcal{K} \setminus \{\pm 2, \pm 2i\sqrt{3}\}$ a due a due diversi

$$b_{j2} = \frac{2b_{j1} + 12}{2 - b_{j1}} \qquad b_{j3} = \frac{2b_{j1} - 12}{2 + b_{j1}}$$

e $6\nu_0 + 4(\nu_1 + \nu_2) + 12 \sum_{j=1}^{m} k_j \equiv 0 \mod q$.

Se $\mathcal{G}_0 = \mathcal{J}_4$, $q=2$, $p=3$

$$(4a') \qquad y^2 = (x^3-x)^{\nu_0}(x^6+x^4+x^2+1)^{\nu_1}\prod_{j=1}^{m}[(x^6+x^4+x^2+1)^4 - a_j(x^3-x)^6]$$

dove $\nu_i \in \{0, 1\}$, $a_1, \ldots, a_m \in \mathcal{K}^*$ a due a due diversi.

Se $\mathcal{G}_0 = \mathcal{J}_4$, $q=2$, $p \geqslant 5$

$$(4a'') \qquad y^2 = (x^5-x)^{\nu_0}[(x^4+1)(x^8-34x^4+1)]^{\nu_1}(x^8+14x^4+1)^{\nu_2} \cdot \prod_{j=1}^{m}[(x^8+14x^4+1)^3 - a_j(x^5-x)^4]$$

dove $\nu_i \in \{0, 1\}$, $a_1, \ldots, a_m \in \mathcal{K}^* \setminus \{108\}$ a due a due diversi.

Se $\mathcal{G}_0 = \mathcal{J}_4$, $q \geqslant 5$, $p=3$

$$(4b') \qquad y^q = (x^3-x)^{\nu_0}(x^6+x^4+x^2+1)^{\nu_1}\prod_{j=1}^{m}[(x^6+x^4+x^2+1)^4 - a_j(x^3-x)^6]^{k_j}$$

dove $0 \leqslant \nu_i < q$, $1 \leqslant k_j < q$, $a_1, \ldots, a_m \in \mathcal{K}^*$ a due a due diversi,
$4\nu_0 + 6\nu_1 + 24\sum_{j=1}^{m} k_j \equiv 0 \mod q$.

Se $\mathcal{G}_0 = \mathcal{J}_4$, $q \geqslant 3$, $p \notin \{2, 3, q\}$

$$(4b'') \qquad y^q = (x^5-x)^{\nu_0}(x^8+14x^4+1)^{\nu_1}[(x^4+1)(x^8-34x^4+1)]^{\nu_2} \cdot \prod_{j=1}^{m}[(x^8+14x^4+1)^3 - a_j(x^5-x)^4]^{k_j}$$

dove $0 \leqslant \nu_i < q$, $1 \leqslant k_j < q$, $a_1, \ldots, a_m \in \mathcal{K}^* \setminus \{108\}$ a due a due diversi,
$6\nu_0 + 8\nu_1 + 12\nu_2 + 24\sum_{j=1}^{m} k_j \equiv 0 \mod q$.

Se $\mathcal{G}_0 = \mathcal{A}_5$, $q=2$, $p=3$

$$(5a') \qquad y^2 = (g_\infty(x))^{\nu_\infty}(g_0(x))^{\nu_0}\prod_{j=1}^{m}[(g_0(x))^6 - a_j(g_\infty(x))^5]$$

dove $\nu_\infty, \nu_0 \in \{0, 1\}$, $a_1, \ldots, a_m \in \mathcal{K}^*$ a due a due diversi.

Se $\mathscr{G}_0 = \mathscr{A}_5$, $q=2$, $p=5$

$$y^2 = (h_\infty(x))^{\nu_\infty}(h_0(x))^{\nu_0}\prod_{j=1}^{m}[(h_0(x))^3 - a_j(h_\infty(x))^{10}] \tag{5a''}$$

dove $\nu_\infty, \nu_0 \in \{0, 1\}$, $a_1, \ldots, a_m \in \mathscr{K}^*$ a due a due diversi.

Se $\mathscr{G}_0 = \mathscr{A}_5$, $q=2$, $p \geq 7$

$$y^2 = (f_0^*(x))^{\nu_0^*}(f_0(x))^{\nu_0}(f_\infty(x))^{\nu_\infty}\prod_{j=1}^{m}[(f_0(x))^3 - a_j(f_\infty(x))^5] \tag{5a'''}$$

dove $\nu_0^*, \nu_0, \nu_\infty \in \{0, 1\}$, $a_1, \ldots, a_m \in \mathscr{K}^* \setminus \{-1728i\}$ a due a due diversi.

Se $\mathscr{G}_0 = \mathscr{A}_5$, $q \geq 3$, $p=2$

$$y^q = (k_\infty(x))^{\nu_\infty}(k_0(x))^{\nu_0}\prod_{j=1}^{m}[(k_0(x))^5 + a_j(k_\infty(x))^{12}]^{k_j} \tag{5b'}$$

dove $\nu_\infty, \nu_0 \in \{0, 1, \ldots, q-1\}$, $1 \leq k_j \leq q-1$, $a_1, \ldots, a_m \in \mathscr{K}^*$ a due a due diversi, $5\nu_\infty + 12\nu_0 + 60\sum_{j=1}^{m} k_j \equiv 0 \mod q$.

Se $\mathscr{G}_0 = \mathscr{A}_5$, $q \geq 5$, $p=3$

$$y^q = (g_\infty(x))^{\nu_\infty}(g_0(x))^{\nu_0}\prod_{j=1}^{m}[(g_0(x))^6 - a_j(g_\infty(x))^5]^{k_j} \tag{5b''}$$

dove $\nu_\infty, \nu_0 \in \{0, 1, \ldots, q-1\}$, $1 \leq k_j \leq q-1$, $a_1, \ldots, a_m \in \mathscr{K}^*$ a due a due diversi, $12\nu_\infty + 10\nu_0 + 60\sum_{j=1}^{m} k_j \equiv 0 \mod q$.

Se $\mathscr{G}_0 = \mathscr{A}_5$, $q=3$ o $q \geq 7$, $p=5$

$$y^q = (h_\infty(x))^{\nu_\infty}(h_0(x))^{\nu_0}\prod_{j=1}^{m}[(h_0(x))^3 - (h_\infty(x))^{10}]^{k_j} \tag{5b'''}$$

dove $\nu_\infty, \nu_0 \in \{0, 1, \ldots, q-1\}$, $1 \leq k_j \leq q-1$, $a_1, \ldots, a_m \in \mathscr{K}^*$ a due a due diversi, $6\nu_\infty + 20\nu_0 + 60\sum_{j=1}^{m} k_j \equiv 0 \mod q$.

Se $\mathscr{G}_0 = \mathscr{A}_5$, $q \geq 3$, $p \notin \{2, 3, 5, q\}$

$$y^q = (f_0^*(x))^{\nu_0^*}(f_0(x))^{\nu_0}(f_\infty(x))^{\nu_\infty}\prod_{j=1}^{m}[(f_0(x))^3 - a_j(f_\infty(x))^5]^{k_j} \tag{5b''''}$$

dove $\nu_0, \nu_0^*, \nu_\infty \in \{0, 1, \ldots, q-1\}$, $1 \leqslant k_j \leqslant q-1$, $a_1, \ldots, a_m \in \mathscr{K}^* \setminus \{1728i\}$ a due a due diversi, $30\nu_0^* + 20\nu_0 + 12\nu_\infty + 60 \sum_{j=1}^{m} \nu_j \equiv 0 \mod q$.

Se $\mathscr{G}_0 = \mathscr{E}_p(m)$

$$y^q = \prod_{j=1}^{s} [(\prod_{b \in \mathscr{U}} (x-b) - a_j]^{k_j} \tag{6}$$

dove $1 \leqslant k_j < q$, $a_1, \ldots, a_s \in \mathscr{K}$ a due a due diversi.

Se $\mathscr{G}_0 = \mathscr{E}_p(m) \times_s \mathscr{C}_n$, $n | p^m - 1$

$$y^q = (d_0(x))^{\nu_0} \prod_{j=1}^{s} [(d_0(x))^n - a_j]^{k_j} \tag{7}$$

dove $0 \leqslant \nu_0 < q$, $1 \leqslant k_j < q$, $a_1, \ldots, a_s \in \mathscr{K}^*$ a due a due diversi.

Se $\mathscr{G}_0 = PSL(2, p^m)$, $p \geqslant 3$, $q = 2$

$$y^2 = (l_\infty(x))^{\nu_\infty} (l_0(x))^{\nu_0} \prod_{j=1}^{k} [(l_0(x))^{(n+1)/2} - a_j (l_\infty(x))^{(n(n-1))/2}] \tag{8a}$$

dove $n = p^m$, $\nu_\infty, \nu_0 \in \{0, 1\}$, $a_1, \ldots, a_k \in \mathscr{K}^* a$ a due a due diversi.

Se $\mathscr{G}_0 = PSL(2, p^m)$, $p \geqslant 3$, $q \geqslant 3$

$$y^q = (l_\infty(x))^{\nu_\infty} (l_0(x))^{\nu_0} \prod_{j=1}^{k} [l_0(x)^{(n+1)/2} - a_j (l_\infty(x))^{(n(n-1))/2}]^{k_j} \tag{8b}$$

dove $\nu_\infty, \nu_0 \in \{0, 1\}$, $a_1, \ldots, a_k \in \mathscr{K}^*$ a due a due diversi,
$\nu_0(n^2-n) + \nu_\infty(n+1) + \frac{1}{2} n(n^2-1) \sum_{j=1}^{k} k_j \equiv 0 \mod q$.

Se $\mathscr{G}_0 = PGL(2, p^m)$, $p \geqslant 3$, $q = 2$

$$y^2 = (l_\infty(x))^{\nu_\infty} (l_0(x))^{\nu_0} \prod_{j=1}^{s} [(l_0(x))^{n+1} - a_j (l_\infty(x))^{n(n-1)}] \tag{9a}$$

dove $\nu_\infty, \nu_0 \in \{0, 1\}$, $a_1, \ldots, a_s \in \mathscr{K}^*$ a due a due diversi.

Se $\mathscr{G}_0 = PGL(2, p^m)$, $p \geqslant 2$, $q \geqslant 3$

$$y^q = (l_\infty(x))^{\nu_\infty} (l_0(x))^{\nu_0} \prod_{j=1}^{s} [(l_0(x))^{n+1} - a_j (l_\infty(x))^{n(n-1)}]^{k_j} \tag{9b}$$

dove $\nu_\infty, \nu_0 \in \{0, 1, q-1\}$, $a_1, \ldots, a_s \in \mathscr{K}^*$ a due a due diversi,

$$\nu_0 n(n-1) + \nu_\infty(n-1) + n(n^2-1)\sum_{j=1}^{s} k_j \equiv 0 \mod q .$$

R. Brandt ha dimostrato, che anche le affermazioni inverse sono vere. Cioè, *se un'estensione* $\mathscr{F}$ *di* $\mathscr{K}$ *ammette un'equazione del tipo* (1), (2a'), ..., (9b), *allora* $\mathscr{F}$ *è un'estensione di Kummer del tipo* $[\mathscr{C}_n|p, q]$, $[\mathscr{D}_n|p, q]$, ..., $[PGL(2, 2^m)|p, q]$, *rispettivamente.*

Bibliografia

[1] R. BRANDT, *Uber die Automorphismengruppen von algebraischen Funktionenkörpern*, Dissertation Univ. Essen, 1988.

[2] R. BRANDT und H. STICHTENOTH, *Die Automorphismengruppen hyperelliptischer Kurven*, Manuscripta Math. **55** (1986).

[3] H. S. M. COXETER and W. O. J. MOSER, *Generators and relations for discrete groups*, Springer, Berlin, 1980.

[4] M. DEURING, *Lectures on the theory of algebraic functions of one variable*, Lecture Notes in Math. **314**, Springer, Berlin, 1973.

[5] A. DUMA, *Sugli automorfismi di superfici di Riemann compatte*, Conf. Sem. Mat. Univ. Bari **207** (1985).

[6] L. GREENBERG, *Maximal groups and signatures*, Ann. of Math. Stud. 79, Princeton Univ. Press, Princeton, N.J., 1973.

[7] P. J. HILTON and U. STAMMBACH, *A course in homological algebra*, Springer, Berlin, 1971.

[8] B. HUPPERT, *Endliche Gruppen* I, Springer, Berlin, 1967.

[9] A. HURWITZ, *Über algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1893).

[10] F. KLEIN, *Über die binären Formen mit linearen Transformationen in sich selbst*, Math. Ann. **9** (1876).

[11] F. KLEIN, *Über die Transformationen der elliptischen Funktionen und die Ausflösung der Gleichung fünften Grades*, Math. Ann. **14** (1879).

[12] F. KLEIN, *Über die Transformationen siebenter Ordnung der elliptischen Functionen*, Math. Ann. **14** (1879).

[13] M. L. MADAN and R. C. VALENTINI, *A Hauptsatz of L. E. Dickson and Artin-Schreier extension*, J. Reine Angew. Math. **318** (1980).

[14] D. J. MADDEN and R. C. VALENTINI, *The groups of automorphisms of algebraic function fields*, J. Reine Angew. Math. **343** (1983).

[15] J. NEUBÜSER, *Die Untergruppenverbände der Gruppen der Ordung* ≤ 100 *mit Aushahme der Ordunngen* 64 *und* 96, Habilitationsschrift Univ. Kiel, 1967.

[16] P. ROQUETTE, *Über die Automorphismen eines algebraischen Funktionenkörpers*, Arch. Math. 3 (1952).

[17] P. ROQUETTE, *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik*, Math. Z. 117 (1970).

[18] J. J. ROTMAN, *An introduction to homological algebra*, Academic Press, New York, 1979.

[19] H. L. SCHMID, *Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, J. Reine Angew. Math. 179 (1938).

[20] J. SCHUR, *Untersuchungen über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. 132 (1907).

[21] U. STAMMBACH, *Homology in group theory*, Lecture Notes in Math. 359, Springer, Berlin, 1973.

[22] H. STICHTENOTH, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, I, II, Arch. Math. 24 (1973).

[23] H. STICHTENOTH, *Zur Realisierbarkeit endlicher Gruppen als Automorphismengruppen algebraischer Funktionenkörper*, Math. Z. 187 (1984).

***