J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

Generation of Galois extensions by matrix roots

To Professor Shôkichi Iyanaga on his 60th birthday

By Shuichi TAKAHASHI

(Received July 12, 1967)

§ 1. Introduction.

Let us recall the Kummer theory. Let k be a field of characteristic 0 containing m-th roots of unity. Then any cyclic group G of order g which divides m has a faithful 1-dimensional representation:

$$G \ni \sigma \to M_\sigma \in k^* = GL(1, k).$$

This verifies the equation:

$$M_\sigma^m = 1 \quad \text{for all} \quad \sigma \in G.$$

Now, if K/k is a cyclic extension with the galois group $G(K/k) = G$, then by Hilbert's theorem 90 there exists an element $x \in K$ such that

$$M_\sigma = x^{\sigma-1} \quad \text{and} \quad K = k(x).$$

By the above equation for M_σ one knows that

$$x^m = a \in k^*.$$

Conversely, any equation of the form

$$x^m = a \in k^*$$

has a solution in the algebraic closure k_a of k, and generates a cyclic extension $K = k(x)$ of k whose galois group has a faithful representation in $\{x \mid x \in k, x^m = 1\}$.

Next consider the case where k is a field of characteristic $p > 0$. Any cyclic group of order p has a faithful representation:

$$G \ni \sigma \to M_\sigma = \begin{bmatrix} 1 & m_\sigma \\ 0 & 1 \end{bmatrix}, \quad m_\sigma \in GF(p).$$

This gives the equation

$$M_\sigma^{-1} M_\sigma^{(p)} = 1 \qquad \text{for all} \quad \sigma \in G$$

where $M^{(p)} = (m_{ij}^p)$. If $G = G(K/k)$ and

$$M_\sigma = X^{\sigma-1},$$

where $X=\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$, $K=k(x)$, then

$$X^{-1}X^{(p)}=A \qquad \text{is a matrix in } k.$$

This is the Artin-Schreier theory and its generalization to the case of an arbitrary group G has been considered by E. Inaba ([1], [2], [3]).

In this paper we consider a generalization of Kummer theory to the case of an arbitrary group G for a field k of characteristic 0.

The group G has always a faithful representation in k:

$$G \ni \sigma \to M_\sigma \in GL(m, k)$$

e. g. a regular representation. Its characters χ_σ, $\sigma \in G$, are algebraic intergers. Hence they satisfy an equation

$$P(\chi_\sigma)-Q(\chi_\sigma)=0,$$

where P, Q are polynomials with non-negative integral rational coefficients. By the theory of representations, two representations

$$P\langle M_\sigma\rangle,\ Q\langle M_\sigma\rangle$$

are equivalent, where $P\langle M_\sigma\rangle$, or $Q\langle M_\sigma\rangle$, is the matrix which is obtained by replacing the variable x by the matrix M_σ, powers by direct products and sums by direct sums. For example, $P(x)=x^2+x+1$ gives a matrix:

$$P\langle M_\sigma\rangle=\begin{bmatrix} M_\sigma\times M_\sigma & 0 & 0\\ 0 & M_\sigma & 0\\ 0 & 0 & 1\end{bmatrix}$$

of degree m^2+m+1.

Now, there is a non-singular matrix C of degree $P(m)=Q(m)$ such that

$$P\langle M_\sigma\rangle C=CQ\langle M_\sigma\rangle \qquad \text{for all } \sigma \in G.$$

If $G=G(K/k)$ and X is a matrix in K satisfying

$$M_\sigma=X^{\sigma-1},$$

then the matrix

$$P\langle X\rangle^{-1}CQ\langle X\rangle=A \qquad \text{is in } k.$$

Let us consider the converse. Consider two polynomials $P(x)$, $Q(x)$ with non-negative integral rational coefficients such that $P(m)=Q(m)$. Then, by a theorem of A. Weil [8], the set

$$\{M \in GL(m, k_a) \mid P\langle M\rangle=CQ\langle M\rangle C^{-1}\}$$

forms a finite group $G(P, Q, C)$. If k is big enough so that all matrices in $G(P, Q, C)$ are in k, we have the following:

THEOREM. *Let K/k be a galois extension whose galois group $G=G(K/k)$ has a faithful representation:*

$$G \ni \sigma \to M_\sigma \in GL(m, k)$$

such that for two polynomials P, Q and for a non-singular matrix C

$$P\langle M_\sigma\rangle = CQ\langle M_\sigma\rangle C^{-1} \qquad \text{holds for all } \sigma \in G.$$

Then there is a non-singular matrix X in K such that

$$X^{\sigma-1} = M_\sigma \quad \text{and} \quad K = k(X) = k(x_{11}, \cdots, x_{mm}).$$

Moreover the matrix

$$A = P\langle X\rangle^{-1} CQ\langle X\rangle$$

is in k.

Conversely, if for two polynomials P, Q and for non-singular matrices C, A the finite group

$$G(P, Q, C)$$

is contained in $GL(m, k)$ and if the matric equation

$$A = P\langle X\rangle^{-1} CQ\langle X\rangle$$

has a solution in k_a, then the field

$$K = k(X)$$

is galoisian over k and its galois group $G=G(K/k)$ has a faithful representation in $G(P, Q, C)$.

Finally, the author would like to thank Professor Y. Kawada for his kind advices: in particular, the publications by Inaba were informed from him.

§ 2. Proof of the theorem.

Any representation

$$G \ni \sigma \to M_\sigma \in GL(m, k)$$

defines a 1-cocycle: $M_{\sigma\tau} = M_\sigma M_\tau$. Hence by a theorem of Speiser ([7] or [6] p. 159) $H^1(G(K/k), GL(m, K)) = 0$, there is a non-singular matrix X in K such that

$$X^{\sigma-1} = M_\sigma \qquad \text{for all } \sigma \in G.$$

From the galois theory, we have $K = k(X)$.

Consider the matrix

$$A = P\langle X\rangle^{-1} CQ\langle X\rangle.$$

For any $\sigma \in G$, one has

$$A^\sigma = P\langle X^\sigma\rangle^{-1}CQ\langle X^\sigma\rangle = P\langle X\rangle^{-1}P\langle M_\sigma\rangle^{-1}CQ\langle M_\sigma\rangle Q\langle X\rangle$$
$$= P\langle X\rangle^{-1}CQ\langle X\rangle = A,$$

i.e. A is in k.

Conversely, suppose that the matric equation

$$A = P\langle X\rangle^{-1}CQ\langle X\rangle$$

is solvable in k_a. For any $\sigma \in G(k_a/k)$,

$$A = P\langle X^\sigma\rangle^{-1}CQ\langle X^\sigma\rangle .$$

Hence, $M_\sigma = X^{\sigma-1}$ satisfies the equation

$$P\langle M_\sigma\rangle^{-1}CQ\langle M_\sigma\rangle = C .$$

i.e. $M_\sigma \in G(P, Q, C)$.

By the hypothesis, $M_\sigma \in GL(m, k)$, hence,

$$X^\sigma = M_\sigma X \qquad \text{is in } k(X) .$$

This proves that $K = k(X)$ is galoisian and that the galois group G is contained in $G(P, Q, C)$.

§ 3. Comments and an example.

By the theorem of A. Weil, the group

$$G(P, Q, C) = \{M \mid P\langle M\rangle C = CQ\langle M\rangle\}$$

is always finite. But, to know a sufficient condition under which

$$G(P, Q, C) \subseteqq GL(m, k)$$

holds will be interesting. There is another more profound question, what finite subgroups of $GL(m, k)$ are of type $G(P, Q, C)$ for suitable P, Q and C?

The solvability of the matric equation

$$A = P\langle X\rangle^{-1}CQ\langle X\rangle$$

in k_a seems to us a very difficult problem. But this was answered to some degree, by A. Weil in [**9**]. With regard to the matric equation $X^{-1}X^{(p)} = A$ its solvability in some extension of k was known to S. Lang ([**4**] or [**5**] p. 119).

Here is an example of our theory. Consider the case where

$$P(x) = x^3 , \qquad Q(x) = x^2 + 2x , \qquad m = 2 ,$$

and

$$C=\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then

$$G(P, Q, C)=\left\{M \mid M=\begin{pmatrix} a & 0 \\ 0 & a^2 \end{pmatrix},\ a^3=1\right\}$$

$$\cup\left\{M \mid M=\begin{pmatrix} 0 & b \\ b^2 & 0 \end{pmatrix},\ b^3=1\right\}.$$

So, if k contains 3rd roots of unity,

$$G(P, Q, C) \subseteqq GL(2, k)$$

and $G(P, Q, C) \cong S_3$, (the symmetric group of 3 letters). If $X=\begin{pmatrix} x & u \\ v & y \end{pmatrix}$, $\Delta=xy-uv \neq 0$, is a solution of the matric equation

$$A=P\langle X\rangle^{-1}CQ\langle X\rangle,$$

then we have

$$\frac{xy+uv}{\Delta^2} \in k, \quad \frac{xv}{\Delta^2} \in k, \quad \frac{yu}{\Delta^2} \in k$$

$$\frac{xu^2+y^2v}{\Delta^2} \in k, \quad \frac{x^2u+yv^2}{\Delta^2} \in k$$

$$\frac{x^3+v^3}{\Delta^2} \in k, \quad \frac{y^3+u^3}{\Delta^2} \in k.$$

Since

$$\frac{1}{\Delta^2}=\frac{\Delta^2}{\Delta^4}=\left(\frac{xy+uv}{\Delta^2}\right)^2-4\frac{xv}{\Delta^2}\frac{yu}{\Delta^2} \in k,$$

one can write the above equations as follows

$$\Delta^2 \in k, \quad xy+uv \in k, \quad xv \in k, \quad yu \in k, \text{ etc...}$$

In particular, $xv=yu=0$ gives all cyclic extensions of degree 3:

$$X=\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, \quad x^3=a \in k, \quad xy=b \in k.$$

And $xy+uv=x^3+v^3=0$ gives all quadratic extensions:

$$X=\begin{pmatrix} x & y \\ -x & y \end{pmatrix}, \qquad x^2=a\in k, \qquad y=b\in k.$$

University of Montreal

References

[1] E. Inaba, On generalized Artin-Schreier equations, Nat. Sci. Rep. Ochanomizu Univ., **13** (1962), 1–13.
[2] E. Inaba, Normal form of generalized Artin-Schreier equations, Nat. Sci. Rep. Ochanomizu Univ., **14** (1963), 1–15.
[3] E. Inaba, Galois extensions associated with generalized Artin-Schreier equations, Nat. Sci. Rep. Ochanomizu Univ., **14** (1963), 41–44.
[4] S. Lang, Algebraic groups over finite fields, Amer. J. Math., **78** (1956), 555–563.
[5] J.-P. Serre, Groupes algébriques et corps de classes, Act. Sci. Ind., No. 1264, Paris, 1959.
[6] J.-P. Serre, Corps locaux, Act. Sci. Ind., No. 1296, Paris, 1962.
[7] A. Speiser, Zahlentheoretische Sätze aus der Gruppentheorie, Math. Zeit., **5** (1919), 1–6.
[8] A. Weil, Une propriété caractéristique des groupes finis de substitutions, C. R. Acad. Sci. Paris, **199** (1934), 180–182.
[9] A. Weil, Généralisation des fonctions abéliennes, J. Math. Pures Appl., **17** (1938), 47–87.