Generation of Galois extensions by matrix roots

To Professor Shokichi 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:

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

This verifies the equation:

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

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

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

By the above equation for $M_{\sigma}$ 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 $k_\alpha$ of $k$, and generates a cyclic extension $K = k(\alpha)$ of $k$ whose galois group has a faithful representation in \{ $x | x \in k, x^m = 1$\}.

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

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

This gives the equation

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

where $M^{(p)} = (m_{\sigma}^p)$. 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

\[
X^{-1}X^{(p)} = A
\]
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 \( k \):

\[
G \ni \sigma \rightarrow M_\sigma \in GL(m, k)
\]
e.g. a regular representation. Its characters \( \chi_\sigma, \sigma \in G \), are algebraic integers. 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 \( M_\sigma \), 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

\[
P(\langle M_\sigma \rangle)C = CQ(\langle M_\sigma \rangle)
\]
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

\[
P(\langle X \rangle^{-1}CQ(\langle X \rangle) = A
\]
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

\[
\{ M \in GL(m, k) : P(\langle M \rangle) = CQ(\langle M \rangle)C^{-1} \}
\]
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 $C$

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

holds for all $\sigma \in G$.

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

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

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 matrix equation

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

has a solution in $k_\sigma$, 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

$$X^{\sigma^{-1}} = M_\sigma \quad \text{for all} \quad \sigma \in G.$$
\[ A^\sigma = P\langle X^\sigma \rangle^{-1}CQ\langle X^\sigma \rangle = P\langle X \rangle^{-1}P\langle M_\sigma \rangle^{-1}CQ\langle M_\sigma \rangle Q\langle X \rangle = P\langle X \rangle^{-1}CQ\langle X \rangle = A, \]

i.e. \( A \) is in \( k \).

Conversely, suppose that the matrix equation

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

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

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

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,

\[ X^\sigma = M_\sigma X \quad \text{is in} \quad k(X). \]

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

\[ G(P, Q, C) = \{ M | P\langle M \rangle C = CQ\langle M \rangle \} \]

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

\[ G(P, Q, C) \subseteq GL(m, k) \]

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 matrix equation

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

in \( k_\sigma \) seems to us a very difficult problem. But this was answered to some degree, by A. Weil in [9]. With regard to the matrix 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

\[ P(x) = x^3, \quad Q(x) = x^2 + 2x, \quad m = 2, \]

and
Generation of Galois extensions by matrix roots

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

Then

\[
G(P, Q, C) = \{ M | M = \begin{pmatrix} a & 0 \\ 0 & a^2 \end{pmatrix}, \ a^3 = 1 \} \cup \{ M | M = \begin{pmatrix} 0 & b \\ b^2 & 0 \end{pmatrix}, \ b^3 = 1 \}.
\]

So, if \( k \) contains 3rd roots of unity,

\[
G(P, Q, C) \subseteq GL(2, k)
\]

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

\[
A = P(X^{-1}CQ(X),
\]

then we have

\[
\frac{xy+uv}{A^2} \in k, \quad \frac{xv}{A^2} \in k, \quad \frac{yu}{A^2} \in k
\]

\[
\frac{xu^2+y^2v}{A^2} \in k, \quad \frac{x^2u+yu^2}{A^2} \in k
\]

\[
\frac{x^3+v^3}{A^2} \in k, \quad \frac{y^3+u^3}{A^2} \in k.
\]

Since

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

one can write the above equations as follows

\[
A^2 \in k, \quad xy+uv \in k, \quad xv \in k, \quad yu \in k, \text{ etc}.
\]

In particular, \( xy = yu = 0 \) gives all cyclic extensions of degree 3:

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

And \( xy+uv = x^3+v^3 = 0 \) gives all quadratic extensions:
\[ X = \begin{pmatrix} x & y \\ -x & y \end{pmatrix}, \quad x^2 = a \in k, \quad y = b \in k. \]

University of Montreal

References