Tôhoku Math. J.
43 (1991), 117–122

REMARK ON BELYI'S PAPER CONCERNING GALOIS EXTENSIONS OF THE MAXIMAL CYCLOTOMIC FIELD WITH CERTAIN LINEAR GROUPS AS GALOIS GROUPS

HISASHI KOJIMA

(Received January 10, 1990, revised April 12, 1990)

Introduction. Recently, using Galois covering of the projective line $\boldsymbol{P}$, Belyi [1] realized certain type of Chevalley groups as the Galois extensions of the maximal abelian extension $\boldsymbol{Q}_{\mathrm{ab}}$ of the rational number field $\boldsymbol{Q}$.

The purpose of this note is to construct Galois extensions of $\boldsymbol{Q}_{\mathrm{ab}}$ having $GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$ and $SL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$ as their Galois groups. This note is a supplement to Belyi's paper [1].

In the preparatory Section 1, we shall discuss the class number of systems of generators of a finite group.

In Section 2, using a modification of Belyi's method in [1], we calculate the class number of a system of 3-generators of $GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$. Furthermore, applying these results, we derive the existence of Galois extensions L and L' of $\boldsymbol{Q}_{\mathrm{ab}}$ such that

$$\mathrm{Gal}(L/\boldsymbol{Q}_{\mathrm{ab}}) \cong GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z}) \qquad \text{and} \qquad \mathrm{Gal}(L'/\boldsymbol{Q}_{\mathrm{ab}}) \cong SL(m, \boldsymbol{Z}/p^n\boldsymbol{Z}) .$$

Belyi's proof is essentially based on arguments on representations of groups and linear algebra over fields. But, in our case, we need to consider representations of groups and linear algebra over the ring $\boldsymbol{Z}/p^n\boldsymbol{Z}$ with zero divisors. In contrast to a matrix over a field, it is difficult to discuss the resolution of eigenspaces and the standard form of a matrix over a non-integral ring. So we use a method slightly different from his to derive our results.

We mention that our results in the case where $m=2$ are contained in the theory of elliptic modular functions. Several natural questions remain open to explore whether there exist Galois extensions of $\boldsymbol{Q}_{\mathrm{ab}}$ with $GL(m, \boldsymbol{Z}_p)$ and $SL(m, \boldsymbol{Z}_p)$ as Galois groups, where $\boldsymbol{Z}_p$ means the ring of p-adic integers, which is a motivation for our study. The author hopes to treat this question on some occasion.

Finally, the author is indebted to the referee suggesting some revisions of this paper.

NOTATION. We denote by $\boldsymbol{Q}$ and $\boldsymbol{Z}$ the rational number field and the ring of rational integers, respectively. $\mathrm{Gal}(L/K)$ means the Galois group of a Galois extension L of a field K.

1. The class number of a system of generators of a group. Let G be a finite group.

For a $g \in G$, we denote by $[g]$ the conjugacy class containing g. For each ordered set $(c_1, \cdots, c_s)$ of conjugacy classes of G, we put

$$C = C(c_1, \cdots, c_s) = \{\tilde{\sigma} = (\sigma_1, \cdots, \sigma_s) \mid \sigma_i \in c_i (i = 1, \cdots, s)\}$$

and call it a class structure of G. Define

$$\Sigma(C) = \{\tilde{\sigma} = (\sigma_1, \sigma_2, \cdots, \sigma_s) \in C \mid \langle \sigma_1, \sigma_2, \cdots, \sigma_s \rangle = G \text{ and } \sigma_1\sigma_2 \cdots \sigma_s = 1\}.$$

and call it a system of s-generators of G with respect to C. The group G acts on $\Sigma(C)$ by conjugation

$$(\tilde{\sigma})^\tau = (\tau^{-1}\sigma_1\tau, \cdots, \tau^{-1}\sigma_s\tau)$$

for all $\tau \in G$ and for all $\tilde{\sigma} = (\sigma_1, \cdots, \sigma_s) \in \Sigma(C)$. We say that $\tilde{\sigma}'$ and $\tilde{\sigma}$ of $\Sigma(C)$ are equivalent to each other if there exists a τ of G satisfying $\tilde{\sigma}' = (\tilde{\sigma})^\tau$. We denote by $\Sigma(C)/\mathrm{Inn}(G)$ the set of all equivalence classes of $\Sigma(C)$. The cardinality of $\Sigma(C)/\mathrm{Inn}(G)$ is called the class number of s-generators of G with respect to C modulo the inner automorphisms and is denoted by $l_G^i(C)$.

2. Calculation of the class number of $GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$**.** We fix an odd prime number p and denote by $\boldsymbol{Z}/p^n\boldsymbol{Z}$ the ring of integers modulo p^n. Let $GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$ (resp. $SL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$) denote the general linear group (special linear group) of degree m over $\boldsymbol{Z}/p^n\boldsymbol{Z}$. Let w be a generator of the multiplicative group $(\boldsymbol{Z}/p^n\boldsymbol{Z})^\times$ of integers modulo p^n prime to p^n. We consider two special elements σ_1 and σ_2 of $GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$ defined by

$$\sigma_1 = \begin{pmatrix} w & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{if } m = 2,$$

$$\sigma_1 = \begin{pmatrix} 1 & 1 & \\ 0 & 1 & 0 \\ & 0 & E_{m-2} \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 0 & \\ \vdots & E_{m-1} \\ 0 & \\ \varepsilon w & 0 \cdots 0 \end{pmatrix} \qquad \text{if } m \geqq 3,$$

where $\varepsilon = (-1)^{m-1}$ and E_i means the unity of $GL(i, \boldsymbol{Z}/p^n\boldsymbol{Z})$. We can prove the following lemma using the method of Matzat [3, pp. 109–110]:

LEMMA 1. *In the notation as above, suppose that p is an odd prime number. Then $GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$ is generated by σ_1 and σ_2.*

Put $M = \boldsymbol{Z}/p^n\boldsymbol{Z}$ and $V^m = \{{}^t(\alpha_1, \cdots, \alpha_m) \mid \alpha_i \in \boldsymbol{Z}/p^n\boldsymbol{Z}\ (1 \leqq i \leqq m)\}$. Then V^m is a free module over M of rank m. Fixing a basis of V^m, we may identify $\mathrm{Aut}_M(V^m)$ with $GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$. We put $G_0 = GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})$. The following lemma is a key to our study.

LEMMA 2. *Let p be an odd prime number. Suppose that an M-submodule W of V^m satisfies $W \nsubseteq \{px \mid \forall x \in V^m\}$ and $g \cdot W \subset W$ for every $g \in G_0$. Then W coincides with V^m.*

Proof. By assumption, there is an element $x_0 = {}^t(x_1, \cdots, x_{i_0}, \cdots, x_m)$ of W such that $p \nmid x_{i_0}$. For every $(\lambda_i) \in M^{m-1}$ and an integer $i>0$, we determine matrices $g(\lambda_1, \lambda_2, \cdots, \lambda_{m-1})$ and g_i by

$$g(\lambda_1, \lambda_2, \cdots, \lambda_{m-1})x = {}^t(x_1, \lambda_1 x_1 + x_2, \lambda_2 x_1 + x_3, \cdots, \lambda_{m-1} x_1 + x_m)$$

and

$$g_i x = {}^t(x_i, x_2, x_3, \cdots, x_{i-1}, \overset{\underset{\smile}{i}}{x_1}, x_{i+1}, x_{i+2}, \cdots, x_m)$$

for every $x = {}^t(x_1, x_2, \cdots, x_m) \in V^m$. Define a matrix g by

$$g = g_i g(\lambda_1, \lambda_2, \cdots, \lambda_{m-1}) g_{i_0}$$

for $\lambda_1, \cdots, \lambda_{m-1}$ of M and an integer $i>0$. Then, for every positive integer i, if we choose suitable elements $\lambda_1, \cdots, \lambda_{m-1}$ of M, then $g x_0$ has the form ${}^t(0, \cdots, 0, \overset{\underset{\smile}{i}}{x_{i_0}}, 0, \cdots, 0)$. This completes our proof.

By some modification of methods of Belyi [1, Theorem 2], we can verify the following theorem. Belyi used essentially arguments on linear algebra over a field, but we use careful analysis on linear algebra over a ring with zero divisors.

THEOREM 1. *If p is an odd prime number, then*

$$l^i_{G_0}(C([\sigma_1], [\sigma_2], [\sigma_1 \sigma_2]^{-1})) = 1 .$$

PROOF. For simplicity, we assume that $m \geqq 3$. Suppose that $G_0 = \langle \sigma'_1, \sigma'_2 \rangle$, $[\sigma_1] = [\sigma'_1]$, $[\sigma_2] = [\sigma'_2]$ and $[\sigma_1 \sigma_2] = [\sigma'_1 \sigma'_2]$. Without loss of generality, we may assume that $\sigma_2 = \sigma'_2$. We put

$$c = \sigma_1 - E_m \qquad \text{and} \qquad c' = \sigma'_1 - E_m ,$$

where E_m is the unit element of $GL(m, \boldsymbol{Z}/p^n \boldsymbol{Z})$. To verify our assertion, it is enough to show that

$$\sigma'_1 = d^{-1} \sigma_1 d \qquad \text{for some } d \in C_{G_0}(\sigma_2) ,$$

where $C_{G_0}(\sigma_2) = \{ g \in G_0 \mid \sigma_2 g = g \sigma_2 \}$.

Now we have

$$\det(tE_m + \sigma_2 + c\sigma_2) = \det(tE_m + \sigma_2 + c'\sigma_2)$$

with a variable t. The matrix $tE_m + \sigma_2$ is an invertible element of $\mathrm{End}_M(V^m \otimes_M M[[t]])$. Moreover, we have

$$(tE_m + \sigma_2)^{-1} = \sigma_2^{-1} - \sigma_2^{-2} t + \sigma_2^{-3} t^2 - \cdots ,$$

where $M[[t]]$ is the ring of formal power series in t over M. Hence we see that

$$\det(E_m + c\sigma_2(tE_m + \sigma_2)^{-1}) = \det(E_m + c'\sigma_2(tE_m + \sigma_2)^{-1}) .$$

A computation yields

$$\det(E_m+cA)=1+\operatorname{tr}(cA) \quad \text{for every} \quad A\in \operatorname{End}_M(V^m\otimes_M M[[t]]) .$$

Consequently, we have

$$\text{(2.1)} \qquad \operatorname{tr}(c\sigma_2^i)=\operatorname{tr}(c'\sigma_2^i) \qquad \text{for every negative integer } i.$$

Since the order of σ_2 is finite, the above equality holds for every integer i. Putting

$$c_1={}^t(1, 0, \cdots, 0) \qquad \text{and} \qquad c_2=(0, 1, 0, \cdots, 0) ,$$

we obtain $c=c_1c_2$.

Now we shall show that $W=M[\sigma_2]c_1$ is a non-zero invariant space under G_0. Put $\alpha=c_2\sigma_2^ic_1$. Since α is a scalar matrix, we have $c\sigma_2^ic_1=\alpha c_1$, which implies $cM[\sigma_2]c_1\subset M[\sigma_2]c_1$. From this, we have $\sigma_1\cdot W\subset W$. So, by Lemma 1, W is invariant under G_0. Hence, by Lemma 2,

$$\text{(2.2)} \qquad V^m=M[\sigma_2]c_1 .$$

Since c and c' are conjugate to each other, there is a $g\in G_0$ satisfying

$$c'=g^{-1}cg .$$

Define matrices c_1' and c_2' by

$$c_1'=g^{-1}c_1 \qquad \text{and} \qquad c_2'=c_2g .$$

Then $c'=c_1'c_2'$. Since $\alpha'=c_2'\sigma_2^ic_1'$ is a scalar matrix, we have $c'\sigma_2^ic_1'=\alpha'c_1'$. This leads to $c'M[\sigma_2]c_1'\subset M[\sigma_2]c_1'$. Consequently, $M[\sigma_2]c_1'$ is invariant under σ_1'. Since σ_1' and σ_2 generate G_0, $M[\sigma_2]c_1'$ is invariant under G_0. By definition, we can easily check

$$c_1'\not\equiv(0, \cdots, 0) \pmod p .$$

Therefore, by Lemma 2, we have

$$\text{(2.3)} \qquad M[\sigma_2]c_1'=V^m .$$

The two equalities (2.2) and (2.3) show that $f(\sigma_2)c_1=c_1'$ and $g(\sigma_2)c_1'=c_1$ for some $f(x)$, $g(x)\in M[x]$. Hence we have $g(\sigma_2)f(\sigma_2)c_1=c_1$. We may put $g(\sigma_2)f(\sigma_2)=h(\sigma_2)$ for some $h(x)=\sum_{l=0}^{m-1}\alpha_lx^l\in M[x]$. It is easy to see that $h(\sigma_2)c_1={}^t(\alpha_0, \alpha_{m-1}\varepsilon w, \alpha_{m-2}\varepsilon w, \cdots, \alpha_2\varepsilon w, \alpha_1\varepsilon w)=c_1={}^t(1, 0, \cdots, 0)$, which implies $h(\sigma_2)=E_m$. Put $d=g(\sigma_2)$. Then we have

$$\text{(2.4)} \qquad dc_1'=c_1 \qquad \text{and} \qquad d\in C_{G_0}(\sigma_2) .$$

By (2.1) and (2.4), we have

$$\text{(2.5)} \qquad \operatorname{tr}(\sigma_2^ic_1(c_2-c_2'd^{-1}))=0 \qquad \text{for every integer } i.$$

This and (2.2) yield

$$\text{(2.6)} \qquad c_2'=c_2d .$$

Consequently, by (2.4) and (2.6), we have $c'=d^{-1}cd$. Thus we have Theorem 1 when $m\geqq 3$. In the remaining case $m=2$, we can also proceed similarly.

By the same method as that of Matzat [3, Bemerkung 2 (p. 111)], we can easily check that

(2.7) $$Z(G_0) \text{ has a complement in } N_{G_0}(\langle\sigma_1\rangle)\,,$$

where $N_{G_0}(\langle\sigma_1\rangle)$ is the normalizer of $\langle\sigma_1\rangle$ in G_0.

Here we quote Theorem 1 in Belyi [1] (cf. [2, Theorem 2]).

THEOREM A. *Let G be a finite group generated by σ_1, σ_2 and σ_3 ($\sigma_1\sigma_2\sigma_3=1$). Let c_i be the conjugacy class containing σ_i ($1\leqq i\leqq 3$). Suppose that $l^i_G(C(c_1, c_2, c_3))=1$ and $Z(G)$ has a complement in $N_G(\langle\sigma_1\rangle)$. Then, there exists a regular Galois extension L of the rational function field $\boldsymbol{Q}_{ab}(t)$ over $\boldsymbol{Q}_{ab}$ satisfying*

$$\mathrm{Gal}(L/\boldsymbol{Q}_{ab}(t))\cong G\,,$$

where $\boldsymbol{Q}_{ab}$ means the maximal abelian extension of $\boldsymbol{Q}$ and, if $\boldsymbol{Q}_{ab}$ is algebraically closed in L, Galois extension $L/\boldsymbol{Q}_{ab}(t)$ is called regular.

Using Theorem 1, (2.7), Theorem A and the same method as in Matzat [3, Folgerung 2 (p. 112)], we have the following (see Matzat [3, p. 111]):

THEOREM 2. *In the notation as above, suppose that p is an odd prime number. Then there exist regular Galois extensions $\tilde{L}$ and $\tilde{L}'$ of $\boldsymbol{Q}_{ab}(t)$ such that*

$$\mathrm{Gal}(\tilde{L}/\boldsymbol{Q}_{ab}(t))\cong GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z}) \qquad \text{and} \qquad \mathrm{Gal}(\tilde{L}'/\boldsymbol{Q}_{ab}(t))\cong SL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})\,.$$

By virtue of the Hilbert irreducibility theorem and Theorem 2, we have the following (cf. [3, p. 218] and [4, p. 362]):

COROLLARY. *Suppose that p is an odd prime number. Then there exist Galois extensions L and L' satisfying*

$$\mathrm{Gal}(L/\boldsymbol{Q}_{ab})\cong GL(m, \boldsymbol{Z}/p^n\boldsymbol{Z}) \qquad \text{and} \qquad \mathrm{Gal}(L'/\boldsymbol{Q}_{ab})\cong SL(m, \boldsymbol{Z}/p^n\boldsymbol{Z})\,.$$

REFERENCES

[1] G. V. BELYI, On Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk. SSSR. Ser. Mat. 43 (1979), 267–276; Math. USSR. Izv. 14 (1980), 247–256.

[2] G. V. BELYI, On extensions of the maximal cyclotomic field having a given classical Galois group, J. reine angew. Math. 341 (1983), 147–156.

[3] B. H. MATZAT, Konstruktive Galoistheorie, Lecture Notes in Math. 1284, Springer-Verlag, Berlin-Heidelberg-New York (1987).

[4] B. H. MATZAT, Rationality criteria for Galois extensions, in Galois groups over $\boldsymbol{Q}$, Proc. of Workshop, March 23–27, 1987 (Y. Ihara, K. Ribet and J.-P. Serre, eds.), Math. Sciences Research Institute Series vol. 16, Springer-Verlag, Berlin-Heidelberg-New York.

Department of Mathematics
The University of Electro-Communication
Chofu-shi, Tokyo 182
Japan