ON GALOIS EXTENSIONS OF A MAXIMAL CYCLOTOMIC FIELD

Изв. Акад. Наук СССР
Сер. Мат. Том 43 (1979), Вып. 2

Math. USSR Izvestija
Vol. 14 (1980), No. 2

ON GALOIS EXTENSIONS OF A MAXIMAL CYCLOTOMIC FIELD

UDC 519.4

G. V. BELYĬ

Abstract. This paper is devoted to the realization of certain types of Chevalley groups as the Galois group of extensions of certain cyclotomic fields. In addition, a criterion for an algebraic curve to be defined over an algebraic number field is given.

Bibliography: 11 titles.

Introduction

No general methods are yet known for constructing a Galois extension over the rational number field $\mathbf{Q}$ having a given unsolvable (e.g., simple) Galois group H. The only cases when such extensions are known to exist are $H = S_n$ (Hilbert), $H = A_n$ (Hilbert, and also in [11] with a simpler proof), and $H = SL(2, p)$ with certain restrictions on the prime p (see [11]). In all of these cases one constructs an extension $K/\mathbf{Q}(t)$ with Galois group H, and the existence of the required extension $L/\mathbf{Q}$ then follows from the Hilbert irreducibility theorem.

It is worth noting that in many cases the absence of certain roots of unity in L leads to essential difficulties in constructing extensions K/L with the given Galois group. Hence, one might suppose that the problem of constructing such extensions becomes much simpler if we limit ourselves to the case when L contains all of the roots of unity, for example, when $L = \mathbf{Q}_{ab}$ is the maximal abelian extension of $\mathbf{Q}$. Thus, in this case the construction of extensions K/L with solvable Galois groups goes through much more simply (see [5]).

The purpose of this paper is to solve the analogous question for certain types of simple groups. Namely, let k be a finite field with q elements, and let H be one of the following groups:

$GL(n, q)$;
$SO(2n+1, q)$, $q \equiv 1\ (2)$;
$CSp(2n, q)$, $q \equiv 1\ (2)$ and $q \neq 9$ for $n \equiv 0\ (2)$;
$U(n, q)$, $q \equiv 1\ (2)$.

We prove that there exists an extension K/L with Galois group H for some abelian extension L of $\mathbf{Q}$. In addition, we solve the same problem for the groups $SL(n, q), PSL(n, q)$,

1980 *Mathematics Subject Classification.* Primary 12A55, 14H25, 14H30; Secondary 12A35, 14E20.

$Sp(2n, q)$, $PSp(2n, q)$, $SU(n, q)$ and $PSU(n, q)$ under the same restrictions on the field k. We do this by constructing coverings of the projective line $\mathbf{P}_1$ with Galois group of the above form which are defined over certain subfields of cyclotomic fields, and we then apply the Hilbert irreducibility theorem. We also indicate how to find the field L which is needed for our construction.

§1. Conditions for descending the ground field

NOTATION. Let $c(B, A)$ be the centralizer and $N(B, A)$ the normalizer of the subset B of the group A, let A' be the commutant of A, let (C, ψ, A) be the semidirect product corresponding to the homomorphism $\psi\colon A \longrightarrow \mathrm{Aut}\, C$, let $\mathfrak{F}$ be the free group with two generators and F its completion with respect to all subgroups of finite index, let $\hat{\mathbf{Z}}$ be the same completion for the ring of integers $\mathbf{Z}$, $\mathbf{C}$ the field of complex numbers, $\bar{\mathbf{Q}}$ the field of all algebraic numbers, $G = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, $\mathscr{U} = \mathbf{P}_1 \setminus \{0, 1, \infty\}$, and $\mathscr{K}$ the maximal extension of the field $\bar{\mathbf{Q}}(t)$ which is unramified outside 0, 1 and ∞.

We consider a finite irreducible unramified covering $X \xrightarrow{\varphi} \mathscr{U}(\mathbf{C})$. By the Riemann existence theorem, we may assume that it is algebraic. If $\sigma \in \mathrm{Aut}(\mathbf{Q}/\mathbf{C})$, then $\deg(\varphi^\sigma) = \deg(\varphi)$. Every such covering corresponds to some subgroup T of the fundamental group $\pi_1(\mathscr{U}(\mathbf{C})) \cong \mathfrak{F}$ of index $\deg(\varphi)$. Since there are only finitely many such subgroups, and the coverings corresponding to the same subgroup are isomorphic, it follows that we can apply Weil's criterion [1] and suppose that φ is defined over the field $\bar{\mathbf{Q}}$.

Thus, we obtain an exact sequence

$$1 \to F \to \mathrm{Gal}(\mathscr{K}/\mathbf{Q}(t)) \to G \to 1, \tag{1}$$

corresponding to the tower $\mathbf{Q}(t) \subset \bar{\mathbf{Q}}(t) \subset \mathscr{K}$. Here the group F has two generators x and y such that the cyclic subgroups $\langle x\rangle$, $\langle y\rangle$ and $\langle xy\rangle$ are the decomposition groups at the points 0, 1 and ∞. They come from the generators of the group $\pi_1(\mathscr{U}(\mathbf{C}))$ corresponding to winding around the omitted points 0 and 1 in some given direction.

LEMMA 1. *All commutative subgroups of F are cyclic.*

PROOF. If M is a commutative but not a cyclic subgroup, then, for some homomorphism $\alpha\colon F \longrightarrow A$ to a finite group A, the image $\alpha(M)$ contains a subgroup $B \cong \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$, where p is some prime number. Let $a, b \in B$ be a pair of generators. For the B-module $C \cong \mathbf{Z}/p\mathbf{Z}$ there exists an extension $0 \longrightarrow C \longrightarrow D \xrightarrow{\beta} B \longrightarrow 0$ such that none of the preimages $\beta^{-1}(a)$ and $\beta^{-1}(b)$ commute. Let $\bar{\beta} \in H^2(B, C)$ be the cocycle corresponding to this extension, let $C' = \mathbf{Z}[A] \otimes_{\mathbf{Z}[B]} C$, and let $\bar{\gamma} \in H^2(A, C')$ be the image of the cocycle $\bar{\beta}$ under the Shapiro isomorphism (see [7], Chapter I, §2.5). Then for the extension $0 \longrightarrow C' \longrightarrow D' \xrightarrow{\gamma} A \longrightarrow 1$, corresponding to the cocycle γ, again none of the preimages $\gamma^{-1}(a)$ and $\gamma^{-1}(b)$ commute. Since the group F is universal, there must exist a homomorphism $\delta\colon F \longrightarrow D'$ such that $\alpha = \gamma\delta$. Consequently, none of the preimages $\alpha^{-1}(a)$ and $\alpha^{-1}(b)$ commute. We have obtained a contradiction.

COROLLARY. *$c(x, F) = \langle x\rangle$, $c(y, F) = \langle y\rangle$ and $c(F, F) = 1$.*

PROOF. $\langle x\rangle$ and $\langle y\rangle$ are maximal cyclic subgroups of the group F, and $c(F, F) = (x, F) \cap c(y, F) = 1$.

We shall henceforth let $\sim$ denote conjugacy in the group.

We set

$$A = \{\sigma \in \operatorname{Aut} F \mid x^\sigma = x^\alpha,\ y^\sigma = y^{\alpha u},\ (xy)^\sigma \sim (xy)^\alpha,\ \alpha \in \hat{\mathbf{Z}}^*,\ u \in F'\}.$$

Since F' is a characteristic subgroup of F, the set A is a subgroup of $\operatorname{Aut} F$. Since $c(x, F) = \langle x\rangle$ and $c(y, F) = \langle y\rangle$, it follows that $A \cap \operatorname{Int} F = 1$.

The sequence (1) is determined (see [6], Chapter XII) by a homomorphism $\kappa\colon G \to \operatorname{Aut} F/\operatorname{Int} F$ and an element in $H^2(G, c(F, F)) = 0$. If $\sigma \in G$, then $\langle x\rangle^\sigma$ is also a decomposition group at 0, and hence $\langle x\rangle^\sigma \sim \langle x\rangle$ and $x^\sigma \sim x^\alpha$, where $\alpha \in \hat{\mathbf{Z}}^*$. Similarly, $y^\sigma \sim y^\beta$ and $(xy)^\sigma \sim (xy)^\gamma$, where $\beta, \gamma \in \hat{\mathbf{Z}}^*$. Taking the quotient group F/F', we see that $\alpha = \beta = \gamma$. Multiplying σ by an inner automorphism, we may assume that $\sigma \in A$. We have thereby lifted the homomorphism κ to a homomorphism $\pi\colon G \to A \subset \operatorname{Aut} F$. Consequently, the extension (1) is a semidirect product:

$$\operatorname{Gal}(\mathscr{K}/\mathbf{Q}(t)) \cong (F, \pi, G).$$

Let the homomorphism $\epsilon\colon A \to \hat{\mathbf{Z}}^*$ be given by setting $x^\sigma = x^{\epsilon(\sigma)}$, and let the epimorphism $\nu\colon G \to \hat{\mathbf{Z}}^*$ be given by setting $\zeta^\sigma = \zeta^{\nu(\sigma)}$ for all roots of unity ζ. Then, if we consider the abelian subextensions of $\bar{\mathbf{Q}}(t)$ in the field $\mathscr{K}$, we see that $\nu = \epsilon\pi$. We hence obtain $\pi(G') \subset \ker \epsilon$.

We introduce the following classes of finite groups.

DEFINITION. $B \in \Gamma' \iff B = \langle a, b\rangle$ and, if $a' \sim a$, $b' \sim b$, $a'b' \sim ab$ and $\langle a', b'\rangle = B$, then there exists an automorphism σ of B such that $a^\sigma = a'$ and $b^\sigma = b'$.

$B \in \Gamma \iff B \in \Gamma'$ and the automorphisms σ are inner.

For $B \in \Gamma'$ we set

$$\Lambda(B, a, b) = \{\alpha \in \hat{\mathbf{Z}}^* \mid a^\alpha \sim a,\ b^\alpha \sim b,\ (ab)^\alpha \sim ab\},$$
$$\Lambda'(B, a, b) = \{\alpha \in \Lambda(B, a, b) \mid a^\alpha = a\}.$$

Let L_B (L'_B) be the subfield of $\bar{\mathbf{Q}}$ corresponding to the subgroup $\nu^{-1}\Lambda(B, a, b)$ (to $\nu^{-1}\Lambda'(B, a, b)$). For brevity we omit the mention of the dependence on the choice of generators a and b. If L is a subfield of $\bar{\mathbf{Q}}$, we let $G(L)$ denote the group $\operatorname{Gal}(\bar{\mathbf{Q}}/L)$.

THEOREM 1. *If $B \in \Gamma'$, then there exists a covering $X \xrightarrow{\varphi} \mathbf{P}_1$ which is unramified except at 0, 1, ∞ and is defined over the field L_B, such that $\operatorname{Gal}(X/\mathbf{P}_1) \cong B$.*

If $B \in \Gamma$, then this covering can be chosen in such a way that all of the automorphisms in $\operatorname{Gal}(X/\mathbf{P}_1)$ are defined over the field $\mathbf{Q}_{ab}$.

If, in addition, $c(B, B)$ is a direct summand in $c(a, B)$ (respectively, in $N(\langle a\rangle, B)$), then these automorphisms are defined over the field L'_B (over L_B).

PROOF. Consider the epimorphism $\tau\colon F \to B$ for which $\tau(x) = a$ and $\tau(y) = b$. If $\sigma \in G(L_B)$, then

$$a' = \tau(x^\sigma) = \tau(x)^{\nu(\sigma)} \sim a, \quad b' = \tau(y^\sigma) \sim \tau(y)^{\nu(\sigma)} \sim b,$$
$$a'b' = \tau((xy)^\sigma) \sim ab, \quad \langle a', b'\rangle = \tau(F) = B.$$

Since $B \in \Gamma'$, σ induces an automorphism on B which leaves $\ker \tau$ invariant. This means that $(\ker \tau, \pi, G(L_B))$ is a subgroup of (F, π, G). If $\mathcal{M}$ is the subfield of $\mathcal{K}$ corresponding to this subgroup, and $X \xrightarrow{\varphi} \mathbf{P}_1$ is a model for the extension $L_B(t) \overset{\varphi^*}{\hookrightarrow} \mathcal{M}$, then this model clearly has the required property. Thus, we have an exact sequence

$$1 \to B \to \mathrm{Gal}(\bar{\mathbf{Q}}(X)/L_B(t)) \to G(L_B) \to 1. \tag{2}$$

If $B \in \Gamma$, then $\sigma \in G(L_B)$ induces on B the automorphism of conjugation by the element $z(\sigma) \in N(\langle a\rangle, B)$. We obtain a crossed homomorphism $z\colon\ G(L_B) \to N(\langle a\rangle, B)/c(B, B)$, whose restriction to $G(L_B')$, by the definition of the field L_B', gives a crossed homomorphism $z'\colon\ G(L_B') \to c(a, B)/c(B, B)$. Let z'' be the restriction of z to G'. The exact sequence (2) splits (see [6], Chapter XII) if $\Delta(z) = 0$, where Δ is the canonical map:

$$H^1(G(L_B),\ N(\langle a\rangle,\ B)/c(B, B)) \xrightarrow{\Delta} H^2(G(L_B),\ c(B, B)).$$

Since the cohomological dimension of the group G' is one (see [7], Chapter II, §§3.3), it follows that $\Delta(z'') = 0$. If $c(B, B)$ is a direct summand in $c(a, B)$ (in $N(\langle a\rangle, B)$), then $\Delta(z') = 0$ $(\Delta(z) = 0)$, and, by our hypotheses, we have

$$\mathrm{Gal}(\mathbf{Q}(X)/\mathbf{Q}_{\mathrm{ab}}(t)) \cong B \oplus G',$$
$$\mathrm{Gal}(\mathbf{Q}(X)/L_B'(t)) \cong B \oplus G(L_B'), \quad \mathrm{Gal}(\mathbf{Q}(X)/L_B(t)) \cong B \oplus G(L_B).$$

Now Theorem 1 follows from Galois theory.

We note that the field L_B is minimal in the sense that all fields of definition of the automorphisms of these coverings must contain it. In addition, it follows from the definition of L_B that it is obtained by adjoining to $\mathbf{Q}$ the values of all of the characters of the group B at the elements a, b, and ab. From the definition of L_B' it follows that $L_B' = L_B(\sqrt[m]{1})$, where $m = \#\langle a\rangle$. Hence both L_B and L_B' are automatically contained in $\mathbf{Q}(\sqrt[n]{1})$ if $n = $ l.c.m. $(\#\langle a\rangle, \#\langle b\rangle, \#\langle ab\rangle)$, and, all the more, if n is the period of the group B.

§2. A criterion for groups of class Γ

Let V be an m-dimensional vector space over an arbitrary field M, let $D = \mathrm{Aut}\ V$, and let H be a finite group with two generators a and b.

THEOREM 2. *If an imbedding $H \hookrightarrow D$ is an irreducible representation and if for some $\xi \in M$ the matrix $a - \xi E$ has rank 1, then $H \in \Gamma'$. If, in addition, $N(H, D) = H \cdot c(H, D)$, then $H \in \Gamma$.*

PROOF. Suppose that $\langle a', b'\rangle = H$, $a' \sim a$, $b' \sim b$, $a'b' \sim ab$, and that $c = a - \xi E$ and $c' = a' - \xi E$ have rank 1. Without loss of generality we may assume that $b' = b$. It suffices to show that $c' = c^d$, where $d \in c(b, D)$. We have

$$\det(tE + \xi b + cb) = \det(tE + \xi b + c'b).$$

If $\xi = 0$, then $m = 1$, or else a would not be invertible. In this case H would be an abelian group and the proof would be trivial. Suppose that $\xi \neq 0$. Then the matrix $tE + \xi b$ is in-

vertible in the ring $\mathrm{End}(V \otimes M[[t]])$, and

$$(tE+\xi b)^{-1}=\xi^{-1}b^{-1}-\xi^{-2}b^{-2}t+\xi^{-3}b^{-3}t^2-\ldots.$$

If r is a matrix of rank 1 over an integral domain, then $\det(E + r) = 1 + \mathrm{tr}(r)$. This becomes obvious if we consider the Jordan normal form of the matrix $E + r$. We have

$$\det(E+cb(tE+\xi b)^{-1})=\det(E+c'b(tE+\xi b)^{-1})$$

and, consequently,

$$\mathrm{tr}(cb^i)=\mathrm{tr}(c'b^i) \tag{3}$$

for all negative integers i. But, since the order of b is finite, this is actually true for all integers i.

Since c has rank 1, we may assume that $c = c_1c_2$, where c_1 and c_2 are linear maps c_1: $M \to V$ and c_2: $V \to M$. Obviously, $M[b]c_1(1)$ is a nonzero invariant subspace for b and c, and hence for H; thus it coincides with V. Since a' and b also generate H, if we similarly set $c' = c_1'c_2'$, we obtain $M[b]c_1'(1) = V$. Consequently there exists an automorphism d of the space V as an $M[b]$-module, i.e. $d \in c(b, D)$, such that $dc_1' = c_1$. Since the equations (3) do not change if we interchange the factors and conjugate c' by d^{-1}, it follows that

$$\mathrm{tr}(b^ic_1(c_2-c_2'd^{-1}))=0$$

for all integers i. But because $M[b]c_1(1) = V$, these equations imply that $c'_2 = c_2d$ and $c^d = c'$.

§4. Verification of the criterion for certain types of Chevalley groups

Suppose that k is a finite field, λ is a generator of the group k^*, $q = \#k$ and $CSp(2n, 2)$ is the subgroup of $GL(2n, q)$ which preserves up to proportionality a certain nondegenerate skew-symmetric form. Let H be one of the groups $GL(n, q)$, $SO(2n + 1, q)$, $CSp(2n, q)$ or $U(n, q)$ with the same restrictions on the field k as in the introduction. Over a finite field all nondegenerate Hermitian forms are equivalent; the same is true for nondegenerate skew-symmetric forms, and also up to proportionality for nondegenerate symmetric forms of odd-dimensional spaces (see [3], Chapter I, §8). Hence, if H is imbedded in the standard way in $D = GL(m, q)$ ($m = n$, $2n + 1$, $2n$ and n, respectively), then we may assume that the maximal torus of H is contained in the subgroup of diagonal matrices of the group D. Because this imbedding is an irreducible representation (see [9], §12), it follows from Schur's lemma (see [8], §2.2, Proposition 3) that $c(H, D) = c(D, D)$ and the form defining H (if there is such a form) is unique up to proportionality.

Let $R = H \cap SL(m, q)$. We shall consider R as a Chevalley group. Let Σ be the root system of R, and let W be its Weyl group. For roots $r, s \in \Sigma$ we set

$$\Theta(r, s)=\{t\in\Sigma \mid t=ir+js,\ i, j\in\mathbf{Z},\ i, j>0\}.$$

If X_r is a generator of the Lie algebra corresponding to the root $r \in \Sigma$, and if $u \in k$, then we set $x_r(u) = \exp(uX_r)$ and $\mathfrak{X}_r = \{x_r(u) \mid u \in k\}$. For $w \in W$ there exists an element $\bar{w}$ in R such that $x_r(u)^{\bar{w}} = x_{w(r)}(\pm u)$ for all r and u (see [10]). Finally, if we are given $h(i) \in k^*$ for $i = 1, \ldots, m$, let h be the diagonal element of D for which $h_{i,i} = h(i)$.

THEOREM 3. *In the group D there exist two elements a and b which generate the group H and are such that for some $\xi \in k$ the matrix $a - \xi E$ has rank 1.*

To prove this, we shall need the following formulas (see [9], §6, and also [10]):

$$(x_r(u),\ x_s(v)) = 1, \quad \text{if} \quad \Theta(r, s) = \varnothing, \tag{4}$$

$$(x_r(u),\ x_s(v)) = x_{r+s}(\rho uv), \text{ where } \rho = \pm \frac{(r+s,\ r+s)}{(r,\ r)}, \quad \text{if} \quad \Theta(r, s) = \{r+s\}, \tag{5}$$

$$(x_r(u)\, x_s(v)) = x_{r+s}(\pm uv)\, x_{2r+s}(\pm u^2 v), \quad \text{if} \quad \Theta(r, s) = \{r+s,\ 2r+s\} \text{ and } (s, s) = 2(r, r). \tag{6}$$

We shall also need the following

PROPOSITION 1 (DICKSON). *Suppose that the elements $u, v \in k^*$ are such that $k = \mathbf{F}_p(uv)$, where $\mathbf{F}_p$ is the prime field, $p \neq 2$, and, if $p = 3$, then $(uv)^2 \neq -1$. Then the group $SL(2, q)$ is generated by the matrices $\begin{bmatrix} 1 & u \\ & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & \\ v & 1 \end{bmatrix}$.*

For the proof, see [2].

COROLLARY. *If u and v are as in Proposition 1, then the subgroup of R generated by $x_r(u)$ and $x_{-r}(v)$ contains the subgroups $\mathfrak{X}_r$ and $\mathfrak{X}_{-r}$.*

PROOF OF THEOREM 3. Let $T = \langle a, b \rangle$ where a and b are elements of H which will be given below. We consider the following cases:

1) $R = SL(2, q)$, $\Sigma = A_1 = \{\pm r\}$.

Let $w(r) = -r$, $h(1) = \lambda$ and $h(2) = 1$. If $k = \mathbf{F}_2$, set $a = x_r(1)$ and $b = \bar{w}$. It is then obvious that $T = R = H = S_3$.

Otherwise set $b = x_r(1)\bar{w} \in R$ and $a = h$. It is easy to verify that $(a, a^{b^{-1}}) = x_r(\mu)$, where $\mu = \lambda^{-1}(\lambda - 1)^2 \neq 0$. But $x_r(\mu)^{a^i} = x_r(\lambda^{-1}\mu)$. We obtain

$$\mathfrak{X}_r \subset T \Rightarrow \bar{w} \in T \Rightarrow \mathfrak{X}_{-r} \subset T \Rightarrow R \subset T,$$

and, since $\det(a) = \lambda$, we have $T = H$.

2) $R = SL(n, q)$, $n > 2$,

$$\Sigma = A_{n-1} = \{e_i - e_j \mid i \neq j,\ i,\ j = 1,\ 2,\ \ldots,\ n\}.$$

Let $w(e_i) = e_{i+1}$ for $i < n$, $w(e_n) = e_1$, $h(1) = \lambda$ and $h(l) = 1$ for $l > 1$. We set $a = x_{e_1 - e_2}(1) \in R$ and $b = \bar{w}h$. We have $a^{b^i} = x_{e_{i+1} - e_{i+2}}(\pm 1)$ for $i < n - 1$, and $a^{b^{n-1}} = x_{e_n - e_1}(\pm\lambda)$. Using (5), we obtain

$$(a, (a^b, (a^{b^2}, (\ldots, (a^{b^{n-3}}, a^{b^{n-2}}) \ldots)) = x_{e_1 - e_n}(\pm 1) \in T.$$

But by the same formula

$$((x_{e_1 - e_2}(\mu),\ x_{e_n - e_1}(\lambda)),\ x_{e_1 - e_n}(1)) = x_{e_1 - e_2}(\pm \lambda\mu) \quad \text{for all} \quad \mu \in k.$$

All of this means that $\mathfrak{X}_{e_1-e_2} \subset T$. Conjugating this inclusion by the element b and taking (5) into account, we find that $\mathfrak{X}_r \subset T$ for all roots r. Consequently, $R \subset T$. Since $\det(b) = \lambda$, we have $T = H$.

3) $R = SO(2n+1, q)$, $q \equiv 1\ (2)$,

$$\Sigma = B_n = \{\pm e_i,\ \pm e_i \pm e_j \mid i \neq j,\ i, j = 1, 2, \ldots, n\}.$$

In this case and the remaining cases let $w(e_i) = e_{i+1}$ for $i < n$ and $w(e_n) = -e_1$. Let $h_1(1) = \lambda^{-1}$, $h_1(2n+1) = \lambda$ and $h_1(l) = 1$ for the remaining l; let $h_2(n+1) = 1$ and $h_2(l) = -1$ for the remaining l. We set $a = h_2$ and $b = x_{e_1}(1)h_1\bar{w}$. We have

$$(a,\ h_1) = (a,\ \bar{w}) = 1, \quad x_{e_1}(1)^a = x_{e_1}(-1) \Rightarrow (a,\ b^{-1}) = x_{e_1}(-2)$$

$$\Rightarrow x_{e_1}(1) \in T \Rightarrow c = h_1\bar{w} \in T.$$

It is easy to verify that

$$x_{e_1}(1)^{c^n} = x_{-e_1}(\pm\lambda) \in T.$$

It follows from Proposition 1 that $\mathfrak{X}_{\pm e_1} \subset T$. Conjugating by c, we obtain the inclusions $\mathfrak{X}_r \subset T$ for all short roots r. But, by (5), these $\mathfrak{X}_r$ generate all of the group R. Since $a, b \in R$, it follows that $T = R = H$.

4) $R = Sp(2n, q)$, $q \equiv 1\ (2)$ and, if n is even, then $q \neq 9$,

$$\Sigma = C_n = \{\pm e_i \pm e_j \mid i,\ j = 1,\ 2,\ \ldots,\ n\}.$$

Let $h(2l+1) = \lambda$ and $h(2l) = 1$. We set $a = x_{2e_1}(\lambda) \in R$, $b = x_{e_{n-1}+e_n}(1)h\bar{w}$. Taking (4) into account, we have $a^{b^n} = x_{-2e_1}(\pm 1)$ for odd n and $a^{b^n} = x_{-2e_1}(\pm\lambda)$ for even n. It follows from Proposition 1 that $\mathfrak{X}_{\pm 2e_1} \subset T$. Taking (4) into account and conjugating by b, we obtain $\mathfrak{X}_{\pm e_i} \subset T$ for $i < n$, and $\mathfrak{X}_{2e_n} \subset T$. Using (6), we obtain

$$x_{-2e_{n-1}}(\mu)^b = x_{-2e_n}(\pm\lambda^{-1}\mu)\, x_{-e_1-e_n}(\pm\lambda^{-1}\mu)\, x_{-2e_1}(\pm\lambda^{-1}\mu).$$

Consequently,

$$y(\mu) = x_{-2e_n}(\pm\mu)\, x_{-e_1-e_n}(\mu) \in T$$

for all $\mu \in k$. Again using (6), we obtain

$$((y(\mu),\ x_{2e_1}(\eta)),\ x_{-2e_1}(\eta^{-1})) = x_{-2e_n}(\pm\mu^2\eta)\, x_{-e_1-e_n}(\mu) \in T$$

for all $\mu, \eta \in k^*$, and hence $\mathfrak{X}_{-2e_n}, \mathfrak{X}_{-e_1-e_n} \subset T$. But it is now easy to obtain the rest of the $\mathfrak{X}_r$ from the subgroups $\mathfrak{X}_{\pm 2e_i}$ for all i, the subgroup $\mathfrak{X}_{-e_1-e_n}$ and the element b, by using (6). Thus, $R \subset T$.

Let θ be the form which defines R. It is well known (see [4]) that, if $c \in H$ preserves this form, then $\det(c) = 1$, and consequently $c \in R$. Together with the fact that $b\theta b^* = \lambda\theta$, this means that $T = H$.

5) $R = SU(2n+1, q)$, $q \equiv 1\ (2)$, $\Sigma = BC_n = B_n \cup C_n$.

Let $q = q'^2$, $h_1(1) = \lambda^{-1}$, $h_1(2n+1) = \lambda^{q'}$, $h_1(l) = 1$ for the remaining l, and let h_2 be the same as in case 3). We set $a = h_2 \in R$ and $b = x_{e_1}(1)h_1\bar{w}$. The proof that

$R \subset T$ is similar to case 3). Since $\det(b) = \lambda^{q'-1}$, it follows that $T = H$.

6) $R = SU(2n, q)$, $q \equiv 1\ (2)$, $\Sigma = C_n$.

Let $h(1) = \lambda^{-1}$, $h(2n) = \lambda^{q'}$ and $h(l) = 1$ for the remaining l. We set $a = x_{2e_1}(1) \in R$ and $b = x_{e_{n-1}+e_n}(1)h\bar{w}$. The proof that $R \subset T$ is similar to case 4). Since $\det(b) = \lambda^{q'-1}$, it follows that $T = H$.

We now show that this imbedding of H in D also satisfies the second condition of Theorem 2.

LEMMA 2. *$N(H, D) = H \cdot c(H, D)$.*

PROOF. If $H = GL(m, q)$, there is nothing to prove. Suppose that $c \ni N(H, D)$, $H = SO(2n + 1, q)$ and θ is the defining form. We have

$$(u^c)\,\theta\,(u^c)^* = \theta \Rightarrow u\,(c\theta c^*)\,u^* = c\theta c^* \Rightarrow c\theta c^* = \eta\theta,$$

where $\eta \in k^*$. Furthermore, $\eta^{2n+1} = \det(c)^2 \Rightarrow \eta = \rho^2$ for some $\rho \in k^* \Rightarrow \rho^{-1}c \in H$.

The other cases are treated similarly.

COROLLARY. $H \in \Gamma$.

LEMMA 3. *Let a and b be chosen as in Theorem 3. Then, except for case 6), $c(H, H)$ is a direct summand in $N(\langle a\rangle, H)$. In case 6) it is a direct summand in $c(a, H)$.*

PROOF. By the choice of a, it has a ξ-eigensubspace V_ξ of codimension 1. This subspace is obviously invariant under the action of $N(\langle a\rangle, H)$. We obtain a homomorphism

$$\tau : N(\langle a\rangle,\ D) \to GL(V/V_\xi) \cong k^*E = c(D,\ D),$$

which gives $c(D, D)$ as a direct summand in $N(\langle a\rangle, D)$.

In cases 1), 2) and 4), we have $c(H, H) = k^*E$, and so we have what we need in these cases.

In case 3), $c(H, H) = 1$, and there is nothing to prove.

In case 5), we have the orthogonal decomposition $V = V_\xi \oplus V_\xi^\perp$ into ± 1-eigensubspaces for a, and these are invariant under the action of $N(\langle a\rangle, H)$. This immediately gives

$$\tau(N(\langle a\rangle, H) \subset \{\mu E \mid \mu \in k,\ \mu^{q'+1} = 1\} = c(H, H),$$

so that we have the lemma in this case as well.

In case 6) we have $\xi = 1$. Let $e_1 \in V \setminus V_\xi$ and $c \in c(a, H)$, and let (α, β) be a non-degenerate skew-hermitian form on V which defines the group H. Then $e_2 = a(e_1) - e_1 \neq 0$, $e_2 \in V_\xi^\pm$ and $(e_1, e_2) \neq 0$. In addition, by the definition of the homomorphism τ we have $c(e_1) = \tau(c)e_1 + e_3$, where $e_3 \in V_\xi$. We have

$$c(e_2) - \tau(c)\,e_2 = (ca - ac)\,(e_1) = 0$$

$$\Rightarrow (e_1, e_2) = (c(e_1),\ c(e_2)) = (\tau(c)\,e_1, \tau(c)\,e_2) = \tau(c)^{q'+1}(e_1, e_2)$$

$$\Rightarrow \tau(c)^{q'+1} = 1 \Rightarrow \tau(c) \in c(H, H).$$

Let $L = L_H$ in all cases except for the sixth, and in the sixth case let $L = L'_H(\sqrt[p]{1})$, where p is the characteristic of the field k.

Summarizing all of the above, we obtain

COROLLARY. *There exists a Galois covering* $X \longrightarrow \mathbf{P}_1$, *unramified outside* $0, 1, \infty$, *such that* $\mathrm{Gal}(X/\mathbf{P}_1) \cong H$ *and the covering and its automorphisms are defined over the field* L.

We note that in Theorem 3 in all of the cases one of the generators a or b was chosen in the group R. Combined with the fact that H/R is cyclic, this means that the curve X^R is a cyclic covering of the line $\mathbf{P}_1$ which is ramified at only two points. Since these points are defined over L, it follows that X^R is isomorphic to $\mathbf{P}_1$ over L. We have thereby obtained a covering $X \longrightarrow X^R \cong \mathbf{P}_1$ with Galois group R which is defined, along with its automorphisms, over L. We now obtain a covering with the simple Galois group $R/c(R, R)$ in the obvious way.

We can now apply the Hilbert irreducibility theorem to obtain field extensions of L whose Galois groups are isomorphic to H, R and $R/c(R, R)$.

§4. Criterion for algebraicity of the ground field

THEOREM 4. *A complete nonsingular algebraic curve* X *defined over a field of characteristic zero can be defined over* $\bar{\mathbf{Q}}$ *if and only if it can cover* $\mathbf{P}_1$ *with ramification over three points.*

PROOF. In one direction this theorem was proved above, if we take these points to be $0, 1, \infty$. But this is not any restriction, since any two triples of points can be taken to one another by a fractional linear transformation. Now suppose that X is defined over $\bar{\mathbf{Q}}$. We choose an arbitrary nonconstant rational function $t \in \bar{\mathbf{Q}}(X)$. It defines a covering of $\mathbf{P}_1$ with ramification over some finite set of points u which are defined over $\bar{\mathbf{Q}}$. If we find polynomials $f_u(t), g_v(t) \in \mathbf{Q}[t]$ such that f_u is ramified over rational points, i.e.

$$f_u(\{\xi \in \bar{\mathbf{Q}} \mid f_u'(\xi) = 0\}) \subset \mathbf{Q},$$

and g_v is only ramified over $0, 1, \infty$, and such that $f_u(u) \subset Q \cup \infty$ and g_v sends to $0, 1, \infty$ a given finite set v of rational points, consisting of the points $f_u(u)$ and the points over which f_u ramifies, then the function $g_v(f_u(t))$ will give us the required covering.

Let $h_1(t)$ be the minimal polynomial over $\mathbf{Q}$ for the set of finite points in the set u, and let $h_{i+1}(t)$ be the minimal polynomial for the set $\{h_i(\xi) \mid h_i'(\xi) = 0\}$. It is clear that $\deg h_{i+1} \leqslant (\deg h_i) - 1$. Consequently, in no more than $\deg h_1$ steps we must obtain a linear polynomial $h_l(t)$. We now take $f_u(t)$ to be the polynomial $h_l(h_{l-1}(\cdots(h_1(t))\cdots))$.

If $g_{v_1}(t)$ has already been constructed, $v = v_1 \cup \{s\}$ and $v_2 = \{0, 1, g_{v_1}(s)\}$, then we can take $g_v(t)$ to be the polynomial $g_{v_2}(g_{v_1}(t))$. Hence it suffices to construct the polynomial $g_{v_3}(t)$ for a set v_3 consisting of three points. Making a linear change of variables, we may assume that $v_3 = \{0, s, 1\}$, where $0 < s < 1$. If $s = m/(m+n)$, where m and n are positive integers, then we set

$$g_{v_s}(t) = \frac{(m+n)^{m+n}}{m^m n^n} t^m (1-t)^n.$$

COROLLARY. *π is a monomorphism.*

PROOF. Suppose that $\sigma \in \ker \pi$, $\sigma \neq 1$, $j \in \bar{\mathbf{Q}}$, $j^\sigma \neq j$, X is an elliptic curve with invariant j, and $X \longrightarrow \mathbf{P}_1$ is the covering whose existence is guaranteed by Theorem 4. Since σ is obviously contained in G', an argument similar to the proof of Theorem 1 leads to a contradiction.

An interesting question arises: Is it possible to describe the image $\pi(G)$ in the group Aut F in group theoretic terms?

In conclusion, the author would like to thank his advisor I. R. Šafarevič for his constant help with the work and his useful remarks during the preparation of this article.

Received 2/AUG/1978

BIBLIOGRAPHY

1. André Weil, *The field of definition of a variety*, Amer. J. Math. 78 (1956), 509–524.
2. Daniel Gorenstein, *Finite groups*, Harper & Row, New York, 1968.
3. Jean A. Dieudonné, *La géométrie des groupes classiques*, 3ieme ed., Springer-Verlag, Berlin and New York, 1971.
4. Carl Ludwig Siegel, *Symplectic geometry*, Amer. J. Math. 65 (1943), 1–86.
5. Kenkichi Iwasawa, *On solvable extensions of algebraic number fields*, Ann. of Math. (2) 58 (1953), 458–572.
6. A. G. Kuroš, *Theory of groups*, 3rd ed., "Nauka", Moscow, 1967; English transl. of 2nd ed., Vols. I, II, Chelsea, New York, 1955, 1956, 1960.
7. Jean-Pierre Serre, *Cohomologie galoisienne*, 2nd ed., Springer-Verlag, Berlin and New York, 1964.
8. ———, *Représentations linéaires des groupes finis*, Hermann, Paris, 1967; English transl., Springer-Verlag, Berlin and New York, 1977.
9. Robert Steinberg, *Lectures on Chevalley groups*, Yale Univ., New Haven, Conn., 1967; Russian transl., "Mir", Moscow, 1975.
10. ———, *Generators for simple groups*, Canad. J. Math. 14 (1962), 277–283.
11. Kuang Yan Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. 207 (1974), 99–120.

Translated by N. KOBLITZ