Tôhoku Math. Journ.
39 (1987), 437-445.

THE GALOIS GROUPS OF THE POLYNOMIALS $x^n + ax^s + b$, II

HIROYUKI OSADA

(Received August 19, 1986)

Introduction. In the previous paper [3], we have shown that the Galois group of a polynomial $f(x) = x^n + ax^s + b$ (with rational integers a and b) over the rational number field $\boldsymbol{Q}$ is isomorphic to the symmetric group S_n of degree n under the following conditions:

(1) $f(x)$ is irreducible over $\boldsymbol{Q}$.

(2) $a = a_0c^n$, $b = b_0c^n$ and $(a_0c(n-s)s, nb_0) = 1$ (relatively prime).

(3) $|D_0(f)|$ is not a square, where

$$D_0(f) = n^n b_0^{n-s} + (-1)^{n-1} s^s (n-s)^{n-s} a_0^n c^{ns}$$

is a factor of the discriminant $D(f)$ of $f(x)$.

(4) $p \| b_0$ for some prime number p.

(5) There exists a prime number q such that $q|s$ and $k < q$ for any positive integer k with $k|n$ and $k < s/2$.

In this paper, we shall first show that the same result holds without the assumption (5) (Theorem 1). Further, we shall show that there exist infinitely many polynomials $x^n + ax^s + p$ satisfying the above conditions (1), (2), (3) and (4) (Theorem 2).

By Hilbert's irreducibility theorem [2], there exist infinitely many Galois extensions with Galois group S_n or A_n for any n. Schur [4, p. 193-194] gave a criterion for the Galois group of a polynomial over $\boldsymbol{Q}$ to be isomorphic to S_n or to A_n. We here give another criterion for the Galois group of a polynomial over $\boldsymbol{Q}$ to be isomorphic to S_n or to A_n (Theorem 3). As another consequence of our results, we can also construct infinitely many polynomials with the Galois groups A_4, A_5 and A_7 (Corollary 3, Corollary 4 to Theorem 3 and Proposition 2). Besides, we give numerical examples of polynomials with Galois group A_7.

The author would like to thank the referee for his valuable advices.

Let $\boldsymbol{Z}$ be the ring of rational integers. Throughout this paper, we shall denote by K, G and $D(f)$ the splitting field, the Galois group and the discriminant of a polynomial $f(x) \in \boldsymbol{Z}[x]$, respectively.

THEOREM 1. *Let $f(x) = x^n + ax^s + b$ be a polynomial in $\boldsymbol{Z}[x]$. Let $a = a_0c^n$ and $b = b_0c^n$. Then the Galois group G is isomorphic to the* *symmetric group* S_n *of degree* n, *if the following conditions are satisfied, where* $D_0(f) = (-1)^{n(n-1)/2}D(f)/b_0^{s-1}c^{n(n-1)} = n^n b_0^{n-s} + (-1)^{n-1}s^s(n-s)^{n-s}a_0^n c^{ns}$:

(1) $f(x)$ *is irreducible over* $\boldsymbol{Q}$.

(2) $a_0c(n-s)s$ *and* nb_0 *are relatively prime, that is,* $(a_0c(n-s)s, nb_0) = 1$.

(3) $|D_0(f)|$ *is not a square.*

(4) $p \| b_0$ *for some prime number* p, *that is,* b_0 *is divisible by* p *and is not divisible by* p^2.

The proof of Theorem 1 is divided into several steps.

PROPOSITION 1. *Let* $f(x)$ *be a monic polynomial of degree* n *in* $\boldsymbol{Z}[x]$. *Let* p *be a prime number and* $\mathfrak{P}$ *a prime ideal in* K *such that* $\mathfrak{P}|p$. *Further, let* $f(x) \equiv x^s\bar{h}(x) \pmod p$, *where* $\bar{h}(x)$ *is a polynomial in* $\boldsymbol{Z}[x]$ *and* s *is a positive integer. Then the inertia group of* $\mathfrak{P}$ *is generated by a cycle of order* s, *if the following conditions are satisfied*:

(1) *The constant term* a_0 *of* $f(x)$ *is divisible by* p *and is not divisible by* p^2.

(2) $\bar{h}(x) \pmod p$ *is a separable polynomial such that* $\bar{h}(0) \not\equiv 0 \pmod p$.

(3) $p \nmid s$.

PROOF. Since $f(x) \equiv x^s\bar{h}(x) \pmod p$ and $\bar{h}(0) \not\equiv 0 \pmod p$, it follows from Hensel's lemma that $f(x) = g(x)h(x)$ in the rational p-adic number field $\boldsymbol{Q}_p$, where $g(x) \equiv x^s \pmod p$ and $h(x) \equiv \bar{h}(x) \pmod p$. Let $K_{\mathfrak{P}}$ be the $\mathfrak{P}$-completion of K. We obtain $K_{\mathfrak{P}}$ from $\boldsymbol{Q}_p$ by adjoining the roots of $f(x)$. Let L be the splitting field of $g(x)$ over $\boldsymbol{Q}_p$. Since $p \| a_0$, $g(x)$ is an Eisenstein polynomial with respect to the prime p. Hence $g(x)$ is irreducible over $\boldsymbol{Q}_p$ and the order of the inertia group T of p in $L/\boldsymbol{Q}_p$ is divisible by s. So the Galois group Z of $L/\boldsymbol{Q}_p$ is transitive as a permutation group on the roots of $g(x)$. Since the Galois group Z is the decomposition group of p in $L/\boldsymbol{Q}_p$, the ramification group V of p in $L/\boldsymbol{Q}_p$ is a normal subgroup of the decomposition group Z of p in $L/\boldsymbol{Q}_p$. The ramification group V is a p-subgroup of the decomposition group Z. Since Z is isomorphic to a subgroup of S_s, V is isomorphic to a p-subgroup of S_s. Since $p \nmid s$, any p-Sylow subgroup of S_s is isomorphic to a p-Sylow subgroup of S_{s-1}. Hence V is isomorphic to a subgroup of S_{s-1}. Thus V is necessarily trivial. Hence the inertia group T of p in $L/\boldsymbol{Q}_p$ is cyclic. Moreover, T is generated by a cycle of order s, since Z is transitive as a permutation group on s letters, while T is cyclic of order divisible by s and is a normal subgroup of Z. Let M be the splitting field of $h(x)$ over $\boldsymbol{Q}_p$. Since $\bar{h}(x) \pmod p$ is a separable polynomial, p is unramified in $M/\boldsymbol{Q}_p$. Hence T is isomorphic to the inertia group of $\mathfrak{P}$. This completes the proof. □

REMARK. When $s = p$ in this Proposition, the inertia group of $\mathfrak{P}$ contains a cycle of order s.

LEMMA 1. *Let $f(x) = x^n + ax^s + b$ be an irreducible polynomial in $\boldsymbol{Z}[x]$, where $a = a_0c^n$, $b = b_0c^n$ and $(a_0c(n-s)s, nb_0) = 1$. Let p be a prime number and $\mathfrak{P}$ a prime ideal in K such that $\mathfrak{P}|p$. If $p \| b_0$, then the inertia group of $\mathfrak{P}$ is generated by a cycle of order s.*

PROOF. From the conditions, $f(x) \equiv x^s(x^{n-s} + a) \pmod p$. Since $p \nmid a(n-s)$, we see that $x^{n-s} + a \pmod p$ is a separable polynomial. Thus, all the conditions in Proposition 1 are satisfied. □

LEMMA 2. *Let p be a prime number and $\mathfrak{P}$ be a prime ideal in K such that $\mathfrak{P}|p$. Further, let $(a_0c(n-s)s, nb_0) = 1$ and $p|D_0(f)$. Then the inertia group of $\mathfrak{P}$ is either trivial or generated by a transposition* (see [3, Lemma 3]).

LEMMA 3. *Let $(cs, nb_0) = 1$. Then all the prime divisors of c are unramified in K.*

PROOF. Since $f(x) = x^n + a_0c^nx^s + b_0c^n$, we have $f(x)/c^n = (x/c)^n + a_0c^s(x/c)^s + b_0$. Put $y = x/c$. Then we have $f(x)/c^n = y^n + a_0c^sy^s + b_0$. Since $(n, s) = 1$, the discriminant of a polynomial $y^n + a_0c^sy^s + b_0$ is equal to $(-1)^{n(n-1)/2}b_0^{s-1}(n^nb_0^{n-s} + (-1)^{n-1}s^s(n-s)^{n-s}a_0^nc^{ns})$. Since $(c, nb_0) = 1$, all the divisors of c are unramified in K. □

LEMMA 4. *Let $(a_0c(n-s)s, nb_0) = 1$ and $s \geqq 2$. For any prime $\mathfrak{P}$ in K, the inertia group T of $\mathfrak{P}$ is isomorphic to a subgroup of S_s. In case $s = 1$, T is either trivial or generated by a transposition.*

PROOF. Let p be a prime number and $\mathfrak{P}$ a prime ideal in K such that $\mathfrak{P}|p$. If $p|b_0$, then $f(x) \equiv x^s(x^{n-s} + a) \pmod p$. Since $p \nmid (n-s)a$, we see that $x^{n-s} + a \pmod p$ is a separable polynomial. So the inertia group T of $\mathfrak{P}$ is isomorphic to a subgroup of S_s. If $p|c \cdot D_0(f)$, then the inertia group T is either trivial or generated by a transposition by Lemmas 2 and 3. □

LEMMA 5. *Let p be a prime number. Suppose a permutation group G on the set $\Omega = \{1, 2, \cdots, n\}$ is generated by cycles of order p. If G is transitive on Ω, then it is primitive on Ω.*

PROOF. Assume that G is imprimitive. Let $\bar{\Omega} = \{\Delta_1, \Delta_2, \cdots, \Delta_m\}$ be a complete nontrivial block system of the imprimitive group G. Let σ be a cycle of order p among the generators in G. Without loss of generality, we can assume that $\sigma = (1, 2, \cdots, p)$ and $1 \in \Delta_1$. Since $|\Delta_i| \geqq 2$ $(1 \leqq i \leqq m)$, $\Delta_i \cap \Delta_j \neq \varnothing$ $(i \neq j)$ and p is a prime number, we have

$1, 2, \cdots, p \in \Delta_1$. Hence for any i $(1 \leqq i \leqq m)$, we have $\sigma(\Delta_i) = \Delta_i$. So for any generator σ of G, we have $\sigma(\Delta_i) = \Delta_i$ for any i $(1 \leqq i \leqq m)$. This contradicts our assumption that G is transitive on Ω. □

LEMMA 6. *Let G be a primitive permutation group on the set $\Omega = \{1, 2, \cdots, n\}$. If G contains a transposition, then it is the symmetric group S_n. If G contains a cycle of order 3, then it is either the alternating group A_n or the symmetric group S_n* (see Wielandt [6, Theorem 13.3]).

By Lemmas 5 and 6, we have:

LEMMA 7. *Let G be a permutation group on the set $\Omega = \{1, 2, \cdots, n\}$. If G is generated by transpositions and is transitive on Ω, then it is the symmetric group S_n. If G is generated by cycles of order 3 and is transitive on Ω, then it is either A_n or S_n.*

LEMMA 8. *Let p be a prime number and G be a primitive permutation group on the set $\Omega = \{1, 2, \cdots, n\}$ with $n \geqq p + 3$. If G contains a cycle of order p, then it is either A_n or S_n* (see Wielandt [6, Theorem 13.9]).

By Lemmas 5 and 8, we have:

LEMMA 9. *Let p be a prime number and G be a permutation group on the set $\Omega = \{1, 2, \cdots, n\}$ generated by cycles of order p with $n \geqq p + 3$. If G is transitive on Ω, then it is either A_n or S_n.*

LEMMA 10. *Let p be a prime number and G be a permutation group on the set $\Omega = \{1, 2, \cdots, p\}$. If G is transitive on Ω, then it is primitive on Ω* (see Wielandt [6, Theorem 8.3]).

PROOF OF THEOREM 1. Since $|D_0(f)|$ is not a square, the Galois group G contains a transposition by Lemma 2. Since $p \| b_0$ for some prime number p, G contains a cycle of order s by Lemma 1. Let H be a subgroup of G generated by all transpositions. It is easy to see that H is a normal subgroup of G. By $H(\alpha)$ we shall denote the set $\{\tau(\alpha) | \tau \in H\}$, where α is a root of $f(x)$. Then $|H(\alpha)| = |H(\beta)| = k$ for any roots α and β of $f(x)$. Hence we have $k | n$. Since G contains a cycle of order s and $(n, s) = 1$, we have $s < k$. Now assume that $k < n$. Since $f(x)$ is irreducible over $\boldsymbol{Q}$, G is transitive as a permutation group on the roots of $f(x)$. So there exists an element σ of G such that $H(\sigma(\alpha)) \neq H(\alpha)$. By Minkowski's theorem, there exists no unramified extension of the field $\boldsymbol{Q}$. Hence the Galois group G is generated by all inertia groups. So we have $\sigma = \tau_1 \tau_2 \cdots \tau_m$ for some $m \in \boldsymbol{Z}$, where τ_i $(1 \leqq i \leqq m)$ is a generator of the inertia group of a prime in K. So there exists some τ_i $(1 \leqq i \leqq m)$ such that $H(\tau_i(\alpha)) \neq H(\alpha)$. By Lemma 4, the inertia group of any prime in K is isomorphic to a subgroup of S_s for $s \geqq 2$ (resp. S_2 for $s = 1$). Hence we have $2k < s$ for $s \geqq 2$, since $|H(\alpha)| = k$ and $(k, s) = 1$. This contradicts the assumption that $s < k$ for $s \geqq 2$. In case $s = 1$, for the same reason we have $2k < s + 1 = 2$. This is also impossible. Therefore we have $k = n$. Hence H is transitive as a permutation group on the roots of $f(x)$. Hence H is isomorphic to S_n by Lemma 7. Therefore G is isomorphic to S_n. □

REMARK. In case $s = 1$ and 2, we do not require the conditions (3) and (4). Further, K is an unramified extension of $Q(\sqrt{D(f)})$ in the narrow sense with A_n as the Galois group (see [3, Corollary 2 to Theorem 1 and Theorem 2]).

EXAMPLE. Let $f(x) = x^5 + 3x + 1$. Then we have $f(x) \equiv (x + 1)(x^4 - x^3 + x^2 - x + 1) \pmod 3$ and $f(\pm 1) \neq 0$. Hence it is clear that $f(x)$ is irreducible over $\boldsymbol{Q}$. So the Galois group of $f(x)$ over $\boldsymbol{Q}$ is isomorphic to S_5 by Theorem 1. Further, $K/Q(\sqrt{D(f)})$ is unramified in the narrow sense, where $D(f) = 65333 = 79 \cdot 827$. On the other hand, the class number of $\boldsymbol{Q}(\sqrt{65333})$ is equal to 1 (see [5]).

THEOREM 2. *Let $f(x) = x^n + ax^s + p$ be a polynomial in $\boldsymbol{Z}[x]$. If $(n, as) = 1$, then there exist infinitely many primes p such that the Galois group of $f(x)$ over $\boldsymbol{Q}$ is isomorphic to S_n.*

PROOF. Since $f(x) = x^n + ax^s + p$ and $(n, as) = 1$, the discriminant is $D(f) = (-1)^{n(n-1)/2} \cdot p^{s-1} \cdot D_0(f)$, where $D_0(f) = n^n p^{n-s} + (-1)^{n-1} s^s (n - s)^{n-s} a^n$. For a moment let us denote $D_0(f)$ by $D_0(p)$. Let p be any prime number such that $1 + |a| < p$, $(p, a(n - s)s) = 1$ and $|D_0(p)| > 1$. By Funakura's lemma (see [3, Lemma 9]), $f(x)$ is irreducible over $\boldsymbol{Q}$. Since $(n, as) = 1$, we have $(np, a(n - s)s) = 1$. Since $|D_0(p)| > 1$, there exists a prime number q such that $q | D_0(p)$. If $q \| D_0(p)$, then all the conditions in Theorem 1 are satisfied. Now assume that $q^2 | D_0(p)$. Since $q | D_0(p)$ and $(np, a(n - s)s) = 1$, we have $(q, a(n - s)snp) = 1$ and $(p, a(n - s)sq) = 1$. We replace p by $p_1 = p + ka(n - s)sq$, where k is a positive integer. Since $(p, a(n - s)sq) = 1$, by Dirichlet's theorem on prime numbers in arithmetic progressions, the Dirichlet density of the primes p_1 satisfying $p_1 \equiv p \pmod{a(n - s)sq}$ is equal to $1/\varphi(a(n - s)sq)$. Hence there exist infinitely many primes p_1 such that $p_1 = p + ka(n - s)sq$ and $(k, q) = 1$. Since $D_0(p_1) = n^n p_1^{n-s} + (-1)^{n-1} s^s (n - s)^{n-s} a^n$ and $q^2 | D_0(p)$, we have $D_0(p_1) \equiv n^n p^{n-s-1} k(n - s)^2 saq \pmod q$. Hence we have $q \| D_0(p_1)$, since $(q, a(n - s)snp) = 1$. So all the conditions in Theorem 1 are satisfied. This completes the proof. □

THEOREM 3. *Let $f(x)$ be a monic polynomial of degree n in $\mathbf{Z}[x]$. Let p_i $(i = 1, 2)$ be prime numbers. Further, let $f(x) \equiv x^{r_i} g_i(x) \pmod{p_i}$ $(i = 1, 2)$, where $g_i(x)$ $(i = 1, 2)$ are polynomials in $\mathbf{Z}[x]$ and r_i $(i = 1, 2)$ are positive integers. Then the Galois group G of $f(x)$ over $\mathbf{Q}$ is either isomorphic to the alternating group A_n or to the symmetric group S_n, if the following conditions are satisfied*:

(1) *$f(x)$ is irreducible over $\mathbf{Q}$.*

(2) *The constant term of $f(x)$ is divisible by p_i and is not divisible by p_i^2 $(i = 1, 2)$.*

(3) *$g_i(x) \pmod{p_i}$ are separable polynomials such that $g_i(0) \not\equiv 0 \pmod{p_i}$ $(i = 1, 2)$.*

(4) *$p_1 \nmid r_1$ and r_2 is a prime number.*

(5) *$r_2 + 3 \leqq n < 2r_1$.*

PROOF. By Proposition 1 and by the conditions (2), (3) and (4), it follows that the Galois group G contains a cycle of order r_i $(i = 1, 2)$. So we can show in the same way as in the proof of Theorem 1 that a subgroup of G generated by all cycles of order r_2 is transitive, from the conditions (1) and $n < 2r_1$. Since $n \geqq r_2 + 3$, G is either isomorphic to A_n or to S_n by Lemma 9. This completes the proof. □

In case r_1 is a prime number, we do not require the condition $p_1 \nmid r_1$. In case $r_2 = 2$ and 3, we do not require the condition $n \geqq r_2 + 3$ by Lemma 7. Further in case $r_2 = 2$, the Galois group G is isomorphic to S_n by Lemma 7.

COROLLARY 1. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial in $\mathbf{Z}[x]$. Let p, q and r be mutually distinct prime numbers. Then the Galois group G of $f(x)$ over $\mathbf{Q}$ is isomorphic to S_n, if the following conditions are satisfied*:

(1) *$p | a_i$ $(0 \leqq i \leqq n-2)$, $p^2 \nmid a_0$ and $p \nmid (n-1)a_{n-1}$.*

(2) *$q | a_i$ $(0 \leqq i \leqq n-1, i \neq 2)$, $q^2 \nmid a_0$ and $q \nmid (n-2)a_2$.*

(3) *$r | a_i$ $(0 \leqq i \leqq n-1)$ and $r^2 \nmid a_0$.*

PROOF. By the condition (3), $f(x)$ is an Eisenstein polynomial with respect to the prime r. Hence $f(x)$ is irreducible over $\mathbf{Q}$. By the conditions (1) and (2), we have $f(x) \equiv x^{n-1}(x + a_{n-1}) \pmod{p}$ and $f(x) \equiv x^2(x^{n-2} + a_2) \pmod{q}$. So it is easy to see that all the conditions in Theorem 3 are satisfied. □

Putting $r_1 = r_2$ (a prime number) in Theorem 3, we have:

COROLLARY 2. *Let $f(x)$ be a monic polynomial of degree n in $\mathbf{Z}[x]$. Let p be a prime number. Further, let $f(x) \equiv x^r g(x) \pmod{p}$, where $g(x)$*

is a polynomial in $Z[x]$ *and* r *is a positive integer. Then the Galois group* G *of* $f(x)$ *over* Q *is either isomorphic to* A_n *or to* S_n, *if the following conditions are satisfied*:

(1) $f(x)$ *is irreducible over* Q.
(2) *The constant term of* $f(x)$ *is divisible by* p *but not by* p^2.
(3) $g(0) \not\equiv 0 \pmod{p}$.
(4) r *is a prime number.*
(5) $r + 3 \leqq n < 2r$, *that is*, $n/2 < r \leqq n - 3$.

In this corollary, from the conditions (4) and (5), we do not require the condition that $g(x) \pmod{p}$ is a separable polynomial. Further in cases $r = 2$ and 3, we do not require the condition $n \geqq r + 3$.

EXAMPLE 1. Put $f(x) = x^8 + 2^3 \cdot 5x^5 + 2 \cdot 3 \cdot 5^4$. Since $f(x)$ is an Eisenstein polynomial with respect to the prime 2, $f(x)$ is irreducible over Q. Since $f(x) \equiv x^5(x^3 + 1) \pmod{3}$, we see that all the conditions in Corollary 2 are satisfied. Since the discriminant is $D(f) = 2^{28} \cdot 3^8 \cdot 5^{28}$, the Galois group of $f(x)$ over Q is isomorphic to A_8.

EXAMPLE 2. Put $f(x) = x^9 - 3^2x^5 + 2 \cdot 3 \cdot 5$. Since $f(x)$ is an Eisenstein polynomial with respect to the prime 3, $f(x)$ is irreducible over Q. Since $f(x) \equiv x^5(x^4 + 1) \pmod{5}$, we see that all the conditions in Corollary 2 are satisfied. Since the discriminant is $D(f) = 2^8 \cdot 3^{22} \cdot 5^8$, the Galois group of $f(x)$ over Q is isomorphic to A_9.

Using Corollary 2, we can construct infinitely many polynomials with the Galois groups A_4 and A_5.

COROLLARY 3. *Let* $f(x) = x^4 + 4x^3 + b$ *be a polynomial in* $Z[x]$. *Then there exist infinitely many integers* b *such that the Galois group of* $f(x)$ *over* Q *is isomorphic to* A_4.

PROOF. Let $b = k^2 + 27$ for any positive integer k such that $k \equiv \pm 2 \pmod{6}$. The discriminant is $D(f) = 2^8b^2(b - 27) = 2^8b^2k^2$. Let p be a prime number such that $p|b$. Since $k \equiv \pm 2 \pmod{6}$, we have $p \geqq 5$ and $p \nmid k$. So we have $|c| \geqq 5$ and $(c, 6k) = 1$ for any integer c such that $c|b$. Now we show that $f(x)$ is irreducible over Q. Since $b = k^2 + 27$ and $k \equiv \pm 2 \pmod{6}$, we have $f(x) \equiv (x - 1)(x^3 - x^2 - x - 1) \pmod{3}$. If $f(x)$ is reducible over Q, then $f(x)$ has a factor of degree 1. But obviously $f(x)$ has no factor of degree 1, since $|c| \geqq 5$ for any integer c such that $c|b$. So $f(x)$ is irreducible over Q. Since $p|b$, we have $p \geqq 5$ and $f(x) \equiv x^3(x + 4) \pmod{p}$. If $p \| b$, then we see that all the conditions in Corollary 2 are satisfied. If $p^2|b$, then we replace b by $b_1 = k_1^2 + 27$, where $k_1 = k + 6p$. Hence we have $b_1 \equiv 2^2 \cdot 3kp \pmod{p^2}$ and $k_1 \equiv \pm 2 \pmod{6}$. Since

$(p, 6k) = 1$, we have $p \| b_1$. Therefore we see that all the conditions in Corollary 2 are satisfied. $\square$

COROLLARY 4. *Let $f(x) = x^5 + 3 \cdot 5^2c^2x^3 + 2 \cdot 3^4 \cdot 5^4bc^4$ be a polynomial in $\boldsymbol{Z}[x]$. Then there exist infinitely many integers b and c such that the Galois group of $f(x)$ over $\boldsymbol{Q}$ is isomorphic to A_5.*

PROOF. Since $f(x) = x^5 + 3 \cdot 5^2c^2x^3 + 2 \cdot 3^4 \cdot 5^4bc^4$, the discriminant is $D(f) = 2^4 \cdot 3^{16} \cdot 5^{18}b^2c^{16}(5^3b^2 + c^2)$. Let z be a rational integer such that $(z, 5)=1$. Let w be a square-free rational integer such that $(w, 2\cdot 3\cdot 5z)=1$. Further, let $b = 2zw$ and $c = z^2 - 5^3w^2$. Then we have $5^3b^2 + c^2 = (z^2 + 5^3w^2)^2$, since $c^2 = (z^2 + 5^3w^2)^2 - 5^3(2zw)^2$. Hence we see that $D(f) = 2^4 \cdot 3^{16} \cdot 5^{18}b^2c^{16}(z^2 + 5^3w^2)^2$, which means that the Galois group G of $f(x)$ over $\boldsymbol{Q}$ is isomorphic to a subgroup of A_5. Now put $y = (2 \cdot 3 \cdot 5 \cdot bc)/x$ and $g(y) = 2^4 \cdot 3 \cdot 5b^4cf(x)/x^5$. Since $(bc, 5) = 1$, $g(y)$ is irreducible over $\boldsymbol{Q}$ by Eisenstein's criterion with respect to the prime 5. So $f(x)$ is irreducible over $\boldsymbol{Q}$. Hence G is transitive as a permutation group on the roots of $f(x)$. Moreover, the degree of $f(x)$ is the prime 5. Therefore G is primitive by Lemma 10. Besides, it is clear that $(w, c) = 1$. Hence we see that all the conditions in Corollary 2 are satisfied, since $b = 2zw$, $(w, 2 \cdot 3 \cdot 5z) = 1$ and w is a square-free integer. $\square$

Further, we construct infinitely many polynomials with the Galois group A_7 as follows.

PROPOSITION 2. *Let $f(x) = x^7 - 5 \cdot 7^2c^2x^5 + 2 \cdot 5^6 \cdot 7^6 \cdot bc^6$ be a polynomial in $\boldsymbol{Z}[x]$. Then there exist infinitely many integers b and c such that the Galois group of $f(x)$ over $\boldsymbol{Q}$ is isomorphic to A_7.*

PROOF. Since $f(x) = x^7 - 5 \cdot 7^2c^2x^5 + 2 \cdot 5^6 \cdot 7^6 \cdot bc^6$, the discriminant is $D(f) = 2^6 \cdot 5^{36} \cdot 7^{38} \cdot b^4c^{36}(c^2 - 7^5b^2)$. Let z be a rational integer such that $(z, 7) = 1$. Let w be a square-free rational integer such that $(w, 2\cdot 5\cdot 7z) = 1$. Further, let $b = 2zw$ and $c = z^2 + 7^5w^2$. Then we have $c^2 - 7^5b^2 = (z^2 - 7^5w^2)^2$, since $c^2 = (z^2 - 7^5w^2)^2 + 7^5(2zw)^2$. Hence we see that $D(f) = 2^6 \cdot 5^{36} \cdot 7^{38} \cdot b^4c^{36}(z^2 - 7^5w^2)^2$, which means that the Galois group G of $f(x)$ over $\boldsymbol{Q}$ is isomorphic to a subgroup of A_7. Now put $y = (2\cdot 5\cdot 7bc)/x$ and $g(y) = 2^6 \cdot 5 \cdot 7b^6c \cdot f(x)/x^7$. Then $g(y)$ is irreducible over $\boldsymbol{Q}$ by Eisenstein's criterion with respect to the prime 7. So $f(x)$ is irreducible over $\boldsymbol{Q}$. Hence G is transitive as a permutation group on the roots of $f(x)$. Moreover, the degree of $f(x)$ is the prime 7. Therefore G is primitive by Lemma 10. Besides, it is clear that $(w, c) = 1$. So we see that all the conditions in Proposition 1 are satisfied, since $b = 2zw$, $(w, 2 \cdot 5 \cdot 7z) = 1$ and w is a square-free integer. Hence G contains a cycle of order 5.

So G is triply transitive (see Wielandt [6, Theorem 13.8]). Then G is either isomorphic to A_7 or to S_7 (see Burnside [1, p. 216]). Therefore G is isomorphic to A_7. $\square$

Now we list some of the pairs (b, c) satisfying the conditions in Proposition 2.

(6, 151264), (12, 151267), (24, 151279), (30, 151288), (48, 151327), (60, 151363), (66, 151384), (78, 151432), (96, 151519), (102, 151552), (114, 151624), (120, 151663), (132, 151747), (138, 151792), (150, 151888), (156, 151939), (174, 152104), (186, 152224), (192, 152287), (204, 152419), (222, 152632), (228, 152707), (240, 152863), (246, 152944), (258, 153112), (264, 153199), (276, 153379), (282, 153472), (300, 153763), (312, 153967), (318, 154072), (330, 154288).

REFERENCES

[1] W. BURNSIDE, Theory of Groups of Finite Order, Cambridge Univ. Press, 1911.

[2] D. HILBERT, Ueber die irreduzibilität ganzen rationalen Funktionen mit ganzzahligen Koeffizienten, J. Reine Angew. Math. 110 (1892), 104-129.

[3] H. OSADA, The Galois groups of the polynomials $x^n + ax^l + b$, J. Number Theory 25 (1987), 230-238.

[4] I. SCHUR, Gesammelte Abhandlungen, Bd III, Springer-Verlag, Berlin, Heidelberg, New York, 1973.

[5] H. WADA, A Table of Ideal Class Numbers of Real Quadratic Fields (in Japanese), Lecture Note in Math. 10 (1981), Sophia Univ., Tokyo.

[6] H. WIELANDT, Finite Permutation Groups, Academic Press, 1964.

DEPARTMENT OF MATHEMATICS
RIKKYO UNIVERSITY
IKEBUKURO, TOKYO 171
JAPAN