

# A class of trinomials with Galois group $S_n^*$

Anuj Bishnoi and Sudesh K. Khanduja<sup>†</sup>

*Department of Mathematics, Panjab University, Chandigarh-160014, India.*

E-mail: anuj.bshn@gmail.com, skhand@pu.ac.in

**Abstract.** A well known result of Schur states that if  $n$  is a positive integer and  $a_0, a_1, \dots, a_n$  are arbitrary integers with  $a_0 a_n$  coprime to  $n!$ , then the polynomial  $f_n(x) = a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \dots + a_1 x + a_0$  is irreducible over the field  $\mathbb{Q}$  of rational numbers. In case each  $a_i = 1$ , it is known that the Galois group of  $f_n(x)$  over  $\mathbb{Q}$  contains  $A_n$ , the alternating group on  $n$  letters. In this paper, we extend this result to a larger class of polynomials  $f_n(x)$  which leads to the construction of trinomials of degree  $n$  for each  $n$  with Galois group  $S_n$ , the symmetric group on  $n$  letters.

**Keywords:** Field theory and polynomials; Galois theory; Non-Archimedean valued fields.

**2000 Mathematics Subject Classification:** 12E05; 11R32; 12J25.

---

\*The paper is to appear in Algebra Colloquium in 2011.

<sup>†</sup>All correspondence may be addressed to this author.

# 1 Introduction

In 1929, Schur [11] proved that the polynomial

$$f_n(x) = a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \dots + a_1 x + a_0, \quad a_i \in \mathbb{Z}, \quad (a_0 a_n, n!) = 1 \quad (1)$$

is irreducible over the field  $\mathbb{Q}$  of rational numbers. In 1930, he further showed that the Galois group of the  $n^{\text{th}}$  Taylor polynomial of the exponential function given by

$$\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \dots + x + 1$$

contains  $A_n$ , the alternating group on  $n$  letters for every  $n$  (see [12]). In this paper, we extend the above mentioned result of Schur to polynomials  $f_n(x)$  defined by (1). Precisely stated, we prove

**Theorem 1.1.** *Let  $n \geq 4$  and  $a_0, a_1, \dots, a_n$  be integers with  $a_0 a_n$  coprime to  $n!$ . Assume that there exists a prime  $p$  not dividing  $a_p$  such that  $\frac{n}{2} < p < n$  if  $n \leq 7$  and  $\frac{n}{2} < p < n - 2$  if  $n \geq 8$ . Then the Galois group of the polynomial  $f_n(x) = a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \dots + a_1 x + a_0$  over  $\mathbb{Q}$  contains  $A_n$  for  $n \neq 6$ .*

It is shown that the above theorem leads to a class of trinomials of degree  $n$  for each  $n$  with Galois group  $S_n$ , the symmetric group on  $n$  letters. Examples of trinomials with Galois group  $S_n$  occur in [1], [7] and [9]. These do not cover the class of trinomials given by the following theorems; moreover our method of constructing such trinomials is quite different.

**Theorem 1.2.** *Let  $n \geq 4$  be an integer and  $p$  be a prime such that  $n/2 < p < n$ , if  $n \leq 7$  and  $n/2 < p < n - 2$  for  $n \geq 8$ . Let  $A, B$  be integers such that  $A$  is not divisible by  $p$  and  $B$  is coprime to  $n!A$ . If the absolute value of  $B^{n-p} + (-1)^{n+1} \left(\frac{n-p}{p}\right)^{n-p} (n!)^p A^n$  is not the square of an integer, then the Galois group of the trinomial  $g_n(x) = x^n + \frac{n!}{p} n A x^p + n! B$  over  $\mathbb{Q}$  is  $S_n$ .*

The following corollaries will be quickly deduced from the above theorem.

**Corollary 1.3.** *Let  $n \geq 4$  and  $p$  be as in the above theorem. Let  $A, B$  be integers such that  $A$  is not divisible by  $p$  and  $B$  is coprime to  $n!A$ . Then the Galois group of the trinomial  $g_n(x) = x^n + \frac{n!}{p} n A x^p + n! B$  over  $\mathbb{Q}$  is  $S_n$ , if one of the following conditions is satisfied.*

(i)  $n$  is even and  $B \not\equiv \pm 1 \pmod{8}$ .

(ii)  $n$  is odd,  $A$  is positive and there exists a prime  $p'$  dividing  $B$  such that  $n!A$  is a quadratic non-residue modulo  $p'$ .

**Corollary 1.4.** *Let  $A$  be an integer not divisible by 35. Then the Galois group of the trinomial  $t_6(x) = x^6 + 864Ax^5 + 720$  is  $S_6$ .*

The theorem stated below to be proved in the last section gives another class of trinomials over  $\mathbb{Q}$  with Galois group  $S_n$ .

**Theorem 1.5.** *Let  $n \geq 4$  be an integer and  $p$  be a prime such that  $n/2 < p < n$ , if  $n \leq 7$  and  $n/2 < p < n - 2$  for  $n \geq 8$ . Let  $A$  and  $B$  be integers such that  $A$  is not divisible by  $p$  and  $B$  is coprime to  $n!$ . Then the following hold*

(i) *If  $n \equiv 2 \pmod{4}$ ,  $n \neq 6$  and  $B^{n-p} > ((n-p)/p)^{n-p}(n!)^p$ , then the Galois group of  $h_n(x) = x^n + \frac{n!}{p}nx^p + n!B$  over  $\mathbb{Q}$  is  $S_n$ .*

(ii) *If  $n \not\equiv 2 \pmod{4}$  and  $(-1)^{\frac{n-1}{2}}A^n < 0$  in case  $n$  is odd, then the Galois group of  $t_n(x) = x^n + \frac{n!}{p}nAx^p + n!$  over  $\mathbb{Q}$  is  $S_n$ .*

## 2 Preliminary results

Let  $K$  be a field equipped with a real valuation  $v$  and let  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  be a polynomial over  $K$  with  $a_0a_n \neq 0$ . Let  $P_i$  stand for the point in the plane having coordinates  $(i, v(a_{n-i}))$  with  $a_{n-i} \neq 0$ ,  $0 \leq i \leq n$ . Let  $\mu_{ij}$  denote the slope of the line joining the points  $P_i$  and  $P_j$  when  $a_{n-i}a_{n-j} \neq 0$ . Let  $i_1$  be the largest index  $0 < i_1 \leq n$  such that

$$\mu_{0i_1} = \min\{\mu_{0j} \mid 0 < j \leq n, a_{n-j} \neq 0\}.$$

If  $i_1 < n$ , let  $i_2$  be the largest index such that  $i_1 < i_2 \leq n$  and

$$\mu_{i_1i_2} = \min\{\mu_{i_1j} \mid i_1 < j \leq n, a_{n-j} \neq 0\}$$

and so on. The Newton polygon of  $f(x)$  with respect to  $v$  is the polygonal line having segments  $P_0P_{i_1}, P_{i_1}P_{i_2}, \dots, P_{i_{k-1}}P_{i_k}$  with  $i_k = n$ .

We shall use the following well known result regarding Newton polygons (see [10, 5.1.F]).

**Theorem 2.A.** *Let  $K$  be a field complete with respect to a real valuation  $v$  and  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  be a polynomial over  $K$  with  $a_0a_n \neq 0$ . Let  $w$  be the extension of  $v$  to the splitting field of  $f(x)$  over  $K$ . Let  $\mu$  be the*

slope of an edge of the Newton polygon of  $f(x)$  with respect to  $v$ . Then there exists a root  $\alpha$  of  $f(x)$  with  $w(\alpha) = \mu$ .

The results stated below regarding transitive subgroups of  $S_n$  will be used in the sequel (see [5, Theorems 5.6.2, 5.7.2] for Theorem 2.B and [13, Lemma 4.4.3] for Theorem 2.C).

**Theorem 2.B.** *Let  $G$  be a transitive subgroup of  $S_n$ ,  $n \geq 8$  which contains a  $p$ -cycle for some prime  $p$  strictly between  $n/2$  and  $n - 2$ . Then  $G$  contains  $A_n$ .*

**Theorem 2.C.** *If a transitive subgroup  $G$  of  $S_n$  contains a transposition and a  $(n - 1)$ -cycle, then  $G = S_n$ .*

We shall use the following result of Swan regarding the discriminant of trinomials (cf. [14, Theorem 2]).

**Theorem 2.D.** *Let  $n > k > 0$  be integers. Let  $d = (n, k)$  and  $n = n_1d$ ,  $k = k_1d$ . Then the discriminant of the trinomial  $f(x) = x^n + ax^k + b$  with coefficients from any field is*

$$(-1)^{\frac{n(n-1)}{2}} b^{k-1} [n^{n_1} b^{n_1-k_1} + (-1)^{n_1+1} (n-k)^{n_1-k_1} k^{k_1} a^{n_1}]^d.$$

Arguing as in the proof of [4, Lemma 3.2.2], the following lemma can be easily proved. Its proof is omitted.

**Lemma 2.E.** *Let  $v$  be a valuation of a field  $K$  and  $P(x)$  be a monic polynomial of degree  $n$  with coefficients from the valuation ring of  $v$  such that the polynomial  $\bar{P}(x)$  obtained by replacing each coefficient of  $P(x)$  by its image in the residue field of  $v$ , is irreducible over the residue field of  $v$ . Let  $\beta$  be a root of  $P(x)$ . Then  $v$  has a unique prolongation  $w$  to  $K(\beta)$ , which is given by  $w(\sum_{j=0}^{n-1} a_j \beta^j) = \min_j \{v(a_j)\}$ ,  $a_j \in K$ . In particular,  $v$  and  $w$  have the same value group.*

The next result (Theorem 2.1) proved here will be used in the proof of Theorem 1.2. It is of independent interest as well. For the proof of Theorem 2.1, we need the following elementary result of valuation theory (see [8, Chap. II, 8.2, 8.5]).

**Theorem 2.F.** *Let  $v$  be a real valuation of a field  $K$  and  $\theta$  be a root of a monic separable irreducible polynomial  $f(x)$  belonging to  $K[x]$  with factorization  $f(x) = f_1(x)f_2(x) \cdots f_r(x)$  into monic irreducible polynomials over the comple-*

tion  $(\widehat{K}, \widehat{v})$  of  $(K, v)$ . Then there are exactly  $r$  prolongations of  $v$  to  $K(\theta)$ . If  $\theta_i$  is a root of  $f_i(x)$  and  $\widetilde{v}$  is the unique prolongation of  $\widehat{v}$  to the algebraic closure of  $\widehat{K}$ , then the valuations  $w_1, w_2, \dots, w_r$  of  $K(\theta)$  defined by

$$w_i\left(\sum_j a_j \theta^j\right) = \widetilde{v}\left(\sum_j a_j \theta_i^j\right), \quad a_j \in K \quad (2)$$

are the prolongations of  $v$  to  $K(\theta)$ . In particular, the value group of the valuation  $w_i$  is same as the value group of the valuation of  $\widehat{K}(\theta_i)$  extending  $\widehat{v}$ .

The corollary stated below, to be used in the sequel, is an immediate consequence of the above theorem and Lemma 2.E.

**Corollary.** *Let the hypothesis and notations be as in the above theorem. Suppose that  $f(x)$  has coefficients in the valuation ring of  $v$ . If some  $f_i(x)$  is such that the polynomial  $\bar{f}_i(x)$  obtained by replacing the coefficients of  $f_i(x)$  modulo the maximal ideal of  $\widehat{v}$ , is irreducible over the residue field of  $\widehat{v}$ , then the value group of  $w_i$  is same as that of  $v$ .*

We now prove

**Theorem 2.1.** *Let  $f(x)$  be a monic irreducible polynomial of degree  $n$  with coefficients from the ring  $\mathbb{Z}$  of integers, having a root  $\theta$ . Let  $q$  be a rational prime which is ramified in  $\mathbb{Q}(\theta)$ . Suppose that  $f(x) \equiv (x - c)^2 \phi_2(x) \cdots \phi_r(x) \pmod{q}$ , where  $(x - c)$ ,  $\phi_2(x), \dots, \phi_r(x)$  are monic polynomials over  $\mathbb{Z}$  which are distinct and irreducible modulo  $q$ . Then the Galois group of  $f(x)$  over  $\mathbb{Q}$  contains a non-trivial automorphism which keeps  $n - 2$  roots of  $f(x)$  fixed.*

*Proof.* Let  $v_q$  denote the  $q$ -adic valuation of  $\mathbb{Q}$  defined by  $v_q(q) = 1$ . By Hensel's Lemma [8, Chap. II, 4.6],  $f(x)$  factors over the field  $\mathbb{Q}_q$  of  $q$ -adic numbers into monic polynomials as  $f_1(x)f_2(x) \cdots f_r(x)$ , where  $f_1(x) \equiv (x - c)^2 \pmod{q}$ ,  $f_i(x) \equiv \phi_i(x) \pmod{q}$  and hence  $f_i(x)$  is irreducible over  $\mathbb{Q}_q$  for  $2 \leq i \leq r$ . Keeping in mind that  $q$  is ramified in  $\mathbb{Q}(\theta)$ , it now follows from Theorem 2.F and its corollary that  $f_1(x)$  is irreducible over  $\mathbb{Q}_q$  and that there is only one prolongation of  $v_q$  to  $\mathbb{Q}(\theta)$  which is ramified; in fact it is the valuation  $w_1$  given by (2). Fix a prolongation  $w$  of  $w_1$  to the splitting field  $L$  of  $f(x)$  over  $\mathbb{Q}$ . Let  $Z_w, T_w$  denote respectively the decomposition field and the inertia field of the extension  $L/\mathbb{Q}$  with respect to  $w$ . Then  $T_w \subsetneq L$ , as  $T_w/\mathbb{Q}$  is unramified with respect to  $w$  but  $L/\mathbb{Q}$  is not so. Claim is that  $T_w$  contains the splitting field of the polynomial  $f(x)/f_1(x)$  over  $Z_w$ . In view of the fact that  $T_w$  is a normal maximal

unramified extension of  $Z_w$  with respect to  $w$  (cf. [8, Chap. II, 9.11]), the claim is proved once we show that for each root  $\theta'$  of  $f(x)/f_1(x)$ , the extension  $Z_w(\theta')/Z_w$  is unramified with respect to  $w$ . Let  $\theta'$  be a root of  $f_i(x)$ ,  $2 \leq i \leq r$ . Note that the polynomial  $f_i(x)$  has coefficients in  $Z_w = L \cap \mathbb{Q}_q$ . Since the residue field of the valuation  $w|_{Z_w}$  is same as that of  $v_q$  and  $f_i(x)$  is an irreducible polynomial modulo  $q$ , it follows from Lemma 2.E that  $Z_w(\theta')/Z_w$  is an unramified extension with respect to  $w$ . Keeping in mind that  $T_w \neq L$ , it is now clear from the claim that the second degree polynomial  $f_1(x)$  is irreducible over  $T_w$ . Hence the non-trivial automorphism of the Galois group of  $L/T_w$  satisfies the desired property.  $\square$

### 3 Proof of Theorem 1.1.

Consider first the case when  $n \geq 8$ . By hypothesis, there exists a prime  $p$  such that  $\frac{n}{2} < p < n - 2$  with  $p$  not dividing  $a_p$ . Claim is that the slope  $\mu$  (say) of the right most edge of the Newton polygon of  $f_n(x)$  with respect to the  $p$ -adic valuation  $v_p$  is  $1/p$ . It is given that  $a_0 a_n$  is coprime to  $n!$  and hence  $v_p(a_0) = v_p(a_n) = 0$ . So  $\mu$  is given by

$$\mu = \max_{1 \leq j \leq n} \left\{ \frac{v_p(a_0) - v_p(a_j/j!)}{n - (n - j)} \right\} = \max_{1 \leq j \leq n} \left\{ \frac{v_p(j!) - v_p(a_j)}{j} \right\}.$$

Since  $\frac{n}{2} < p < n - 2$ ,  $v_p(j!) = 0$  for  $1 \leq j < p$  and  $v_p(j!) = 1$  for  $p \leq j \leq n$ . Keeping in mind the hypothesis  $v_p(a_p) = 0$ , we conclude that  $\mu = 1/p$ . This proves the claim.

Let  $L$  denote the splitting field of  $f_n(x)$  over  $\mathbb{Q}$ . Let  $\tilde{v}_p$  denote the unique prolongation of the  $p$ -adic valuation of the field  $\mathbb{Q}_p$  of  $p$ -adic numbers to the algebraic closure of  $\mathbb{Q}_p$ . It is immediate from the claim and Theorem 2.A that  $f_n(x)$  will have a root  $\alpha$  in the splitting field  $L\mathbb{Q}_p$  of  $f_n(x)$  over  $\mathbb{Q}_p$  with  $\tilde{v}_p(\alpha) = 1/p$ . It now follows that  $p$  divides the index of ramification and hence the degree of  $L\mathbb{Q}_p/\mathbb{Q}_p$  which divides the degree of  $L/\mathbb{Q}$ . Therefore by Cauchy's Theorem of finite groups, the Galois group  $G$  (say) of  $L/\mathbb{Q}$  has an element of order  $p$ , which must be a  $p$ -cycle as  $p > n/2$ . Also  $G$  is transitive being the Galois group of an irreducible polynomial. It now follows in view of Theorem 2.B that  $G$  contains  $A_n$  for  $n \geq 8$ .

For  $n = 4$ , by hypothesis 3 does not divide  $a_3$ . It can be easily seen that the slope of the right most edge of the Newton polygon of  $f_4(x)$  with respect to  $v_3$

is  $1/3$ . So arguing as above, we see that 3 divides the order of  $G$  and hence 12 divides the order of  $G$  which implies that  $G$  contains  $A_4$ .

In the case  $n = 5$ , keeping in mind the hypothesis that 3 does not divide  $a_3$ , it can be easily seen that the slope of the right most edge of the Newton polygon of  $f_5(x)$  with respect to  $v_3$  is  $1/3$ . So arguing as in the case  $n = 4$ , we see that 15 divides the order of  $G$ . The theorem is proved in this case because  $A_5$  and  $S_5$  are the only transitive subgroups of  $S_5$  whose order is divisible by 15 (see [2, Appendix A]). In the case  $n = 7$ , considering the slope of the right most edge of the Newton polygon of  $f_7(x)$  with respect to  $v_5$  and arguing as in the previous cases, it can be seen that 35 divides the order of  $G$ . Since the only transitive subgroups of  $S_7$  having order divisible by 35 are  $A_7$  and  $S_7$  (cf. [2, Appendix A]), the theorem is proved in this case also.

## 4 Proof of Theorem 1.2 and Corollaries 1.3, 1.4.

*Proof of Theorem 1.2.* Let  $\theta$  be a root of the polynomial  $g_n(x)$  which is irreducible over  $\mathbb{Q}$  in view of [11]. Let  $K$  denote the field  $\mathbb{Q}(\theta)$  and  $d_K$  its discriminant. As is well known the discriminant  $D(g_n(x))$  of  $g_n(x)$  and the index  $i(\theta)$  of  $\mathbb{Z}[\theta]$  in the ring of algebraic integers of  $K$  satisfy

$$D(g_n(x)) = (i(\theta))^2 d_K. \quad (3)$$

Applying Theorem 2.D, we have

$$D(g_n(x)) = (-1)^{\frac{n(n-1)}{2}} n^n (n!)^{n-1} B^{p-1} [B^{n-p} + (-1)^{n+1} \frac{(n-p)^{n-p}}{p^{n-p}} (n!)^p A^n]. \quad (4)$$

Claim is that there exists a prime  $q$  which divides  $d_K$  and  $q$  does not divide  $n!AB$ . In view of (3), (4) and the fact that  $B$  is coprime to  $n!A$ , the claim is proved once we show that the absolute value of  $d'$  defined by

$$d' = B^{n-p} + (-1)^{n+1} \frac{(n-p)^{n-p}}{p^{n-p}} (n!)^p A^n \quad (5)$$

is not a perfect square in  $\mathbb{Z}$ , which is true by virtue of the hypothesis. It now follows from the claim and Dedekind Theorem [6, p. 158, Corollary 3] characterizing ramified primes that  $q$  is ramified in  $K$ .

We next show that

$$g_n(x) \equiv (x-c)^2 \phi_2(x) \cdots \phi_r(x) \pmod{q} \quad (6)$$

where  $c \in \mathbb{Z}$  and  $\phi_i(x)$  ( $2 \leq i \leq r$ ) are monic polynomials with coefficients in  $\mathbb{Z}$ , which are distinct and irreducible modulo  $q$ . Let  $\bar{g}_n(x)$  denote the polynomial obtained by replacing each coefficient of  $g_n(x)$  by its image in  $\mathbb{Z}/q\mathbb{Z}$ . Since  $D(g_n(x)) \equiv 0 \pmod{q}$ , the polynomial  $\bar{g}_n(x)$  has a multiple root in the algebraic closure of  $\mathbb{Z}/q\mathbb{Z}$ , say  $\xi$ . As  $g'_n(x) = x^{p-1}(nx^{n-p} + n!nA)$  and  $n!AB$  is not divisible by  $q$ , it follows that  $\xi^{n-p}$  is the class of  $-n!A$  modulo  $q$ . Hence  $\xi$  is unique and it belongs to  $\mathbb{Z}/q\mathbb{Z}$ . This proves (6).

Keeping in mind that  $q$  is ramified in  $K$  and (6), it follows immediately from Theorem 2.1 that the Galois group  $G$  of  $g_n(x)$  over  $\mathbb{Q}$  contains a transposition. As  $G$  already contains  $A_n$  for  $n \neq 6$  by virtue of Theorem 1.1, we see that  $G = S_n$ . For the case  $n = 6$ , in view of Theorem 2.C it is enough to show that  $G$  contains a 5-cycle. By the hypothesis of this case,  $p = 5$  does not divide  $A$ . A simple calculation shows that the right most edge of the Newton polygon of  $g_6(x)$  with respect to the 5-adic valuation has slope  $1/5$ . So 5 divides the order of  $G$ . Therefore by Cauchy's Theorem,  $G$  contains an element of order 5, which must be a 5-cycle and hence  $G = S_6$  in the present case.  $\square$

*Proof of Corollary 1.3.* Let  $d'$  be as in (5). Assume that (i) holds. Keeping in mind that  $n - p$  is odd and  $n \geq 4$ , it is clear that  $d' \equiv B \not\equiv \pm 1 \pmod{8}$  and so  $|d'|$  cannot be a square in  $\mathbb{Z}$  which proves the result in this case by virtue of Theorem 1.2. If (ii) holds, then  $d' > 0$  and the Legendre symbol  $\left(\frac{d'}{p'}\right) = \left(\frac{n!A}{p'}\right) = -1$  by hypothesis. Hence the corollary follows.  $\square$

*Proof of Corollary 1.4.* Note that  $t_6(x) = x^6 + \frac{6!}{5}6Ax^5 + 6!$  is a polynomial of the form given in Theorem 1.2 with  $n = 6$ ,  $p = 5$  and  $B = 1$ . As in the proof of Corollary 1.3, we need to show that  $|d'| = (6!)^4 4! 6A^6 - 1$  is not a square in  $\mathbb{Z}$ . Since  $A^6 \equiv 1 \pmod{7}$  by Fermat's Theorem, it follows that  $|d'| \equiv 3 \pmod{7}$  and hence not a square modulo 7.  $\square$

## 5 Proof of Theorem 1.5.

Since the polynomial  $h_n(x)$ ,  $n \neq 6$  satisfies the hypothesis of Theorem 1.1, it is irreducible over  $\mathbb{Q}$  and its Galois group contains  $A_n$ . To prove assertion (i), in view of [3, Theorem 7.4.1(b)], it is enough to show that the discriminant of  $h_n(x)$



is negative. Using Theorem 2.D, the discriminant of  $h_n(x)$  is

$$(-1)^{\frac{n(n-1)}{2}} n^n (n!)^{n-1} B^{p-1} [B^{n-p} + (-1)^{n+1} \frac{(n-p)^{n-p}}{p^{n-p}} (n!)^p]$$

which can be easily checked to be negative using the hypothesis. Arguing similarly and verifying that the discriminant of  $t_n(x)$  is

$$(-1)^{\frac{n(n-1)}{2}} n^n (n!)^{n-1} [1 + (-1)^{n+1} \frac{(n-p)^{n-p}}{p^{n-p}} (n!)^p A^n] < 0,$$

assertion (ii) of the theorem follows.

### References.

- [1] S. D. Cohen, A. Movahhedi and A. Salinier, Galois Groups of Trinomials, *J. Algebra* 222 (1999) 561-573.
- [2] John H. Conway, Alexander Hulpke and John McKay, On transitive permutation groups, *LMS J. Comput. Math.* 1 (1998) 1-8.
- [3] David A. Cox, *Galois Theory*, John Wiley & Sons, Inc., New Jersey, 2004.
- [4] A. J. Engler and A. Prestel, *Valued Fields*, Springer-Verlag, Berlin, 2005.
- [5] M. Hall, *The Theory of Groups*, The Macmillan Company, New York, 1959.
- [6] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers* (3rd edn.), Springer-Verlag, Berlin Heidelberg, 2004.
- [7] E. Nart and N. Vila, Equations of the type  $x^n + ax + b$  with absolute Galois group  $S_n$ , *Rev. Univ. Santander.* 2 II (1979) 821-825.
- [8] G. Neukirch, *Algebraic Number Theory*, Springer-Verlag, New York, 1999.
- [9] H. Osada, The Galois groups of polynomial  $x^n + ax^l + b$ , *J. Number Theory* 25 (1987) 230-238.
- [10] P. Ribenboim, *The Theory of Classical Valuations*, Springer-Verlag New York, 1999.
- [11] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen I, *Gesammelte Abhandlungen*, Band III 64 (1929) 140-151.
- [12] I. Schur, Gleichungen ohne Affekt, *Gesammelte Abhandlungen*, Band III 67 (1930) 191-197.
- [13] J. P. Serre, *Topics in Galois Theory*, A. K. Peters Ltd., Wellesley, 2008.
- [14] R. G. Swan, Factorization of polynomials over finite fields, *Pacific J. Math.* 12 (1962) 1099-1106.