

## Square-Free Discriminants and Affect-Free Equations

Kenzo KOMATSU

*Keio University*

### §1. Square-free discriminants.

Unramified  $A_n$ -extensions of quadratic number fields are discussed by Uchida [5], [6] and Yamamoto [10]. Their results are closely related to the fact that there are infinitely many algebraic number fields  $K$  of degree  $n$  ( $n > 1$ ) with the following properties:

1. The Galois group of  $\bar{K}/\mathcal{Q}$  is the symmetric group  $S_n$ , where  $\bar{K}$  denotes the Galois closure of  $K/\mathcal{Q}$ .
2. The discriminant of  $K$  is square-free.

It is the purpose of the present paper to discuss square-free discriminants and affect-free (affektlos) equations. We begin by proving the following theorem. The Galois closure of  $K/\mathcal{Q}$  means the minimal Galois extension of  $\mathcal{Q}$  which contains  $K$ .

**THEOREM 1.** *Let  $K$  denote an algebraic number field of degree  $n$  ( $n \geq 1$ ) and let  $\bar{K}$  denote the Galois closure of  $K/\mathcal{Q}$ . Suppose that the discriminant  $d$  of  $K$  is square-free. Then we have:*

1. *The Galois group of  $\bar{K}/\mathcal{Q}$  is the symmetric group  $S_n$ .*
2. *The Galois group of  $\bar{K}/\mathcal{Q}(\sqrt{d})$  is the alternating group  $A_n$ .*
3. *Every prime ideal is unramified in  $\bar{K}/\mathcal{Q}(\sqrt{d})$ .*

**PROOF.** We may assume that  $n > 1$ . Let  $G$  denote the Galois group of  $\bar{K}/\mathcal{Q}$ . Then  $G$  is a transitive permutation group on  $\{1, 2, \dots, n\}$ . Suppose that  $K$  has a subfield  $F$  such that

$$\mathcal{Q} \subset F \subset K, \quad F \neq \mathcal{Q}, \quad F \neq K.$$

Let  $d_F$  denote the discriminant of  $F$ . Then  $d$  is divisible by  $d_F^m$ , where  $m = [K : F]$  ([1], Satz 39). Since  $m > 1$ , by Minkowski's theorem we see that  $d$  cannot be square-free. This implies that  $G$  is primitive ([9], Theorem 7.4). Let  $p$  denote a prime number which divides  $d$ ; by hypothesis  $d$  is exactly divisible by  $p$ . Then (van der Waerden [7]) the prime ideal decomposition of  $p$  (in  $K$ ) is of the form