L'Enseignement Mathématique, t. 37 (1991), p. 17-30

PRIMES OF DEGREE ONE AND ALGEBRAIC CASES OF ČEBOTAREV'S THEOREM

by H. W. LENSTRA, JR. and P. STEVENHAGEN

ABSTRACT. Let $A \subset B$ be an extension of Dedekind domains for which the corresponding extension of fields of fractions is finite and separable. It is shown that the class group of B is then generated by classes of primes of degree one with respect to A. When the main argument of the proof is applied to the situation of the ray class groups occurring in class field theory, it leads to purely algebraic proofs of special cases of Čebotarev's density theorem.

1. INTRODUCTION

Let A be a Dedekind domain with field of fractions K, and suppose L is a finite field extension of K. Then the integral closure of A in L is a Dedekind domain B, and for each non-zero prime ideal $\mathfrak{q}$ of B we define its *degree* over A as the degree of the residue class field extension at $\mathfrak{q}$, i.e.

$$\deg_A \mathfrak{q} = [B/\mathfrak{q} : A/(A \cap \mathfrak{q})] \ .$$

We write Cl_B for the ideal class group of B and denote the class of $\mathfrak{q}$ in Cl_B by $[\mathfrak{q}]$. Using this notation, we prove the following theorem.

THEOREM 1. *If L/K is a separable field extension and S is a finite set of primes of B, one has*

$$Cl_B = \langle [\mathfrak{q}] : \deg_A \mathfrak{q} = 1 \quad \text{and} \quad \mathfrak{q} \notin S \rangle \ .$$

In case B is not a principal ideal domain, it follows that B has infinitely many primes that are of degree one over A. We will see in section 3 that the hypothesis that L/K be separable cannot be omitted.

1980 Mathematics subject classification (1985): 11R44, 13F05.

Acknowledgements: The authors are supported by the National Science Foundation under grants No. DMS-8706176 and 9002939 and by the Netherlands Organisation for Scientific Research (NWO).