2. The separable case

2. THE SEPARABLE CASE

In this section we will prove the theorems 1 and 2. The proof will depend on the fact that the extension of fields under consideration is separable. In section 3 we will construct examples of inseparable extensions for which the conclusion of theorem 1 does not hold.

Suppose that we are in the situation of theorem 1. As we assume L/K to be separable, there is an element $\alpha \in B$ such that $L = K(\alpha)$. Moreover, there exists $d \neq 0$ in A such that the subring $A[\alpha]$ of B satisfies $dB \subset A[\alpha] \subset B$. For instance, one can take for d the discriminant of the irreducible polynomial of α over K. One has $B_{\mathfrak{p}} = A_{\mathfrak{p}}[\alpha]$ for the localizations at all primes $\mathfrak{p} \nmid dA$, and for a prime $\mathfrak{q}$ in B that lies over such a $\mathfrak{p}$, the element α mod $\mathfrak{q}$ generates the residue class field $B/\mathfrak{q}$ over $A/\mathfrak{p}$.

Both theorem 1 and 2 are easy consequences of the following lemma.

LEMMA. *Choose $d \neq 0$ in A such that $dB \subset A[\alpha]$, and let $\mathfrak{q}$ be a prime of B that does not divide dB. If $\deg_A \mathfrak{q} = f > 1$, then there exists a non-zero element $x \in B$ satisfying*

(a) $x \equiv 1 \bmod dB$

(b) $Bx = \mathfrak{q} \cdot \prod_{i=1}^{t} \mathfrak{b}_i$, *where $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$ are primes of B of degree $< f$ that are coprime to dB.*

If, in addition, a finite number of embeddings ϕ of B into the field of real numbers are given, then the element $x \in B$ can be chosen such that $\phi(x) > 0$ for each of these embeddings.

Proof. Let $\mathfrak{p} = \mathfrak{q} \cap A$, and set $\beta = d\alpha$. As $\mathfrak{q} \nmid dB$, one has $B_{\mathfrak{p}} = A_{\mathfrak{p}}[\beta]$ and Kummer's theorem [12, Ch. I §8] implies that there exist $u_0, u_1, \ldots, u_{f-1} \in A$ such that

$$\mathfrak{q} = \mathfrak{p}B + (\beta^f + u_{f-1}\beta^{f-1} + \ldots + u_1\beta + u_0)B \,. \tag{1}$$

We may assume that

$$x' = \beta^f + u_{f-1}\beta^{f-1} + \ldots + u_i\beta + u_0 \in \mathfrak{q} - \mathfrak{q}^2 \,. \tag{2}$$

This follows from (1) if $\mathfrak{p} \subset \mathfrak{q}^2$, and can otherwise be achieved by adding an element of $\mathfrak{p} - \mathfrak{q}^2$ to u_0, if necessary. We shall obtain the required element

$$\begin{aligned} x = \beta^f + v_{f-1}\beta^{f-1} + u_{f-2}\beta^{f-2} + u_{f-3}\beta^{f-3} + \ldots + u_3\beta^3 \\ + u_2\beta^2 + u_1\beta + v_0 \end{aligned} \tag{3}$$

by modifying the "coefficients" u_{f-1} and u_0 of x'. Our first condition

$$v_0 \equiv 1 \bmod dA \tag{4}$$

will guarantee that $x \in \beta B + v_0 \subset d\alpha B + dA + 1 \subset dB + 1$, as required in (a). The second condition

$$\begin{aligned} v_0 &\equiv u_0 \bmod \mathfrak{p}^2 \\ v_{f-1} &\equiv u_{f-1} \bmod \mathfrak{p}^2 \end{aligned} \tag{5}$$

implies that $x \in \mathfrak{q} - \mathfrak{q}^2$, so $x \neq 0$ and we have

$$xB = \mathfrak{q} \cdot \prod_{i=1}^{t} \mathfrak{b}_i$$

for certain prime ideals $\mathfrak{b}_i \neq \mathfrak{q}$ that do not divide dB. Note also that we cannot have $\mathfrak{b}_i \mid \mathfrak{p}B$, since this would imply that $\mathfrak{b}_i \supset \mathfrak{p}B + xB = \mathfrak{q}$.

We will impose an extra condition on each of v_0 and v_{f-1} to ensure that

$$\deg_A \mathfrak{b}_i < f \qquad (i = 1, \ldots, t) .$$

Let $g \in A[X]$ be the irreducible polynomial of β over K, and M the splitting field of g over K. Denote by C the integral closure of A in M. Then g splits completely as a product $\prod_{j=1}^{n}(X - \beta_j)$ in $C[X]$. Let the finite set $W \subset C$ consist of all sums of f distinct terms from $\beta_1, \beta_2, \ldots, \beta_n$:

$$W = \{ \textstyle\sum_{j \in J} \beta_j : J \subset \{1, 2, \ldots, n\} , \# J = f \} .$$

Our condition on v_{f-1} reads

$$-v_{f-1} \notin W . \tag{6}$$

The ring A is infinite, so we can find v_{f-1} satisfying (5) and (6). Given such an element v_{f-1}, we define a non-zero element

$$y = \prod_{w \in W} (w + v_{f-1}) ,$$

which lies in A as it is a symmetric expression in the roots of g, and require that

(7) $v_0 \equiv 0 \bmod \mathfrak{a}$ for each prime $\mathfrak{a} \mid yA$ of A that does not divide $d\mathfrak{p}$.

There are only finitely many prime divisors of yA, so there exists v_0 satisfying (4), (5) and (7) by the Chinese remainder theorem.

We will now show that our conditions on v_0 and v_{f-1} imply $\deg_A \mathfrak{b}_i < f$ for each prime $\mathfrak{b}_i$ occurring in the decomposition of xB. Fix such a prime,

and put $\mathfrak{a}_i = A \cap \mathfrak{b}_i$ and $\bar{\beta} = \beta \bmod \mathfrak{b}_i$. We have $B/\mathfrak{b}_i = (A/\mathfrak{a}_i)[\bar{\beta}]$ because $\mathfrak{b}_i \nmid dB$. Reduction of (3) modulo $\mathfrak{b}_i$ shows that $\bar{\beta}$ satisfies an f-th degree equation

$$0 = \bar{\beta}^f + \bar{v}_{f-1}\bar{\beta}^{f-1} + \bar{u}_{f-2}\bar{\beta}^{f-2} + \bar{u}_{f-3}\bar{\beta}^{f-3} + \ldots + \bar{u}_3\bar{\beta}^3 + \bar{u}_2\bar{\beta}^2 + \bar{u}_1\bar{\beta} + \bar{v}_0 , \tag{8}$$

so we certainly have $\deg_A \mathfrak{b}_i \leqslant f$. In order to arrive at a contradiction, suppose that equality occurs for our prime $\mathfrak{b}_i$. Then the polynomial

$$\bar{h} = X^f + \bar{v}_{f-1}X^{f-1} + \bar{u}_{f-2}X^{f-2} + \bar{u}_{f-3}X^{f-3} + \ldots + \bar{u}_3X^3 + \bar{u}_2X^2 + \bar{u}_1X + \bar{v}_0$$

is the irreducible polynomial of $\bar{\beta}$ in $(A/\mathfrak{a}_i)[X]$. Since $\bar{\beta}$ is also a zero of $\bar{g} = g \bmod \mathfrak{a}_i[X]$, $\bar{h}$ divides $\bar{g}$ in $(A/\mathfrak{a}_i)[X]$, hence also in $(C/\mathfrak{c}_i)[X]$, where $\mathfrak{c}_i$ is a prime in C lying over $\mathfrak{b}_i$. In $(C/\mathfrak{c}_i)[X]$, the polynomial $\bar{g}$ splits completely as a product $\prod_{j=1}^{n}(X - \bar{\beta}_j)$, with $\bar{\beta}_j = \beta_j \bmod \mathfrak{c}_i$. It follows that $\bar{h} = \prod_{j\in J}(X - \bar{\beta}_j)$, with $J \subset \{1, 2, \ldots, n\}$ of cardinality f. Comparing coefficients at X^{f-1}, we find that $\bar{v}_{f-1} = -\sum_{j\in J}\bar{\beta}_j$. By definition of y, we now have

$$y = \prod_{w\in W}(w + v_{f-1}) \in \mathfrak{c}_i \cap A = \mathfrak{a}_i .$$

As $\mathfrak{a}_i \nmid d\mathfrak{p}$, we have $v_0 \equiv 0 \bmod \mathfrak{a}_i$ by (7). It follows that the irreducible polynomial $\bar{h} \in (A/\mathfrak{a}_i)[X]$ is divisible by X. This contradicts the fact that $\deg h = f > 1$.

We finally have to show that the element $x \in B$ constructed above can be made positive at a finite number of real embeddings $B \rightarrowtail \mathbf{R}$. This follows immediately from the fact that (4), (5) and (7) remain valid when we replace x by $x + k^2$, where k is a suitable element in $yd\mathfrak{p}$. This finishes the proof of the lemma.

Proof of theorem 1. By the approximation theorem, the class group of B is generated by the primes outside S. Thus, let $\mathfrak{q}$ be an ideal of B of degree $\deg_A \mathfrak{q} = f$ that is not in S. We are done if we can show that $[\mathfrak{q}]$ is in the subgroup C of Cl_B that is generated by the classes of primes of degree one that are not in S.

Use induction on f. For $f = 1$ there is nothing to prove, so take $f > 1$. If we choose the element d in the lemma divisible by all primes in S it follows that there exist primes $\mathfrak{b}_i$ outside S with $\deg_A \mathfrak{b}_i < f$ such that $[\mathfrak{q}]$

$= \prod_{i=1}^{t} [\mathfrak{b}_i]^{-1} \in Cl_B$. By our induction hypothesis, all $[\mathfrak{b}_i]$ are in C. It follows that $[\mathfrak{q}]$ is in C. □

By applying the first half of the proof of the lemma to a prime $\mathfrak{q}$ of degree $f = 1$, one can obtain an element $x = \beta + v_0 \in B$ whose ideal factorization reads $xB = \mathfrak{q} \cdot \prod_{i=1}^{t} \mathfrak{b}_i$ for certain primes $\mathfrak{b}_i$ of degree one outside S. It follows that the inverse class $[\mathfrak{q}]^{-1} \in Cl_B$ is a product of classes of primes of degree one outside S. Thus the classes of the primes of degree one outside S generate Cl_B already as a *monoid,* i.e. without using their inverse classes.

It is not true that every ideal class of B necessarily contains a prime of degree one with respect to A. As a trivial counterexample, with $A = B$, one can a take a Dedekind domain that is not principal and invert all prime ideals in the principal class. There are no prime ideals in the principal class of the resulting Dedekind domain. Less trivial examples are found in [6, Ch. III § 15].

Proof of theorem 2. We now take $A = \mathbf{Z}$ and B the ring of integers of F. The possibility of choosing the element x in the lemma in such a way that it is positive under certain embeddings in the field of real numbers and congruent to 1 modulo any given ideal of A shows that the lemma can also be used to generate relations in $Cl_{\mathfrak{f}}$. The proof is further analogous to that of theorem 1. □

Remark. Theorem 2 can be generalized to the case that F is a function field over a finite field. In that case, there is neither a canonical choice for a ring of integers $A \subset F$ nor an absolute degree of the primes of A with respect to a base ring $\mathbf{Z}$. For each non-empty finite set of primes T of F, one can take A to be the intersection of valuation rings $\bigcap_{\mathfrak{p} \notin T} A_{\mathfrak{p}} \subset F$. One defines a *conductor* of A to be a pair consisting of an integral ideal $\mathfrak{f}$ of A and an open subgroup H of finite index in the product of the completions $\prod_{\mathfrak{p} \in T} F_{\mathfrak{p}}^*$ of F. The ray *class group* of A modulo such a conductor is defined as the group of fractional A-ideals that is generated by all primes $\mathfrak{p} \nmid \mathfrak{f}$ of A modulo the subgroup of principal ideals $A\alpha$ for which $\alpha \equiv 1 \bmod^* \mathfrak{f}$ and $\alpha \in H$ under the natural embedding. If k is the field of constants of F and x is an element of $F \setminus k$, one can consider the degree of primes of A with respect to $k(x)$ and show that ray class groups of A are generated by the classes of primes that are of degree one in this sense. The details are left to the reader.

3. The inseparable case

In this section we will show that the separability assumption in theorem 1 cannot be omitted. As we need examples of Dedekind domains having a non-