Modules With Integral Discriminant Matrix

Thesis by

Donald Eugene Maurer

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California 91109

1969

(Submitted April 7, 1969)

Acknowledgements

I wish to thank my advisor, O. Taussky Todd, for suggesting the problem studied in this thesis, and for her patience and encouragement in its preparation. I am also grateful to Dr. D. Estes and Dr. H. Kisilevsky for helpful conversations. Finally, I would like to thank Professor A. Garsia and Professor R. Dean for their encouragement.

The research for this thesis was carried out, in part, while the author was a National Science Foundation Graduate Fellow.

Abstract

Let F be a field which admits a Dedekind set of spots (see O'Meara, Introduction to Quadratic Forms) and such that the integers $\mathbb{Z}_F$ of F form a principal ideal domain. Let $K|F$ be a separable algebraic extension of F of degree n. If M is a $\mathbb{Z}_F$-module contained in K, and $\sigma_1, \sigma_2, \ldots, \sigma_n$ is a $\mathbb{Z}_F$-basis for M, the matrix $D(\underline{\sigma}) = (\text{trace}_{K|F}(\sigma_i\sigma_j))$ is called a discriminant matrix. We study modules which have an integral discriminant matrix. When F is the rational field, we are able to obtain necessary and sufficient conditions on $\det D(\underline{\sigma})$ in order that M be properly contained in a larger module having an integral discriminant matrix. This is equivalent to determining when the corresponding quadratic form

$$f = \sum_{i,j} a_{ij}x_ix_j \qquad (a_{ij} = a_{ji}),$$

with integral matrix (a_{ij}) can be obtained from another such form, with larger determinant, by an integral transformation.

These two main results are then applied to characterize normal algebraic extensions K of the rationals in which $\mathbb{Z}_K$ is maximal with respect to having an integral discriminant matrix.

I. Introduction

Let $K|F$ be a separable algebraic extension of a field F of degree n. For each $\alpha \in K$, the trace of α over F will be denoted by $S_{K|F}(\alpha)$. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a basis for $K|F$, and $\lambda \in K$, then $D_\lambda(\underline{\alpha})$ will denote the $n \times n$ F-matrix $(S_{K|F}(\lambda \alpha_i \alpha_j))$. Matrices of this type have appeared in the work of Faddeev [5], Taussky [11] and Bender [2] in connection with representations. In the special case $\lambda = 1$, the matrix $D(\underline{\alpha}) = (S_{K|F}(\alpha_i \alpha_j))$ is called a discriminant matrix. Taussky [13] has studied the characteristic roots of discriminant matrices when $K|F$ is an algebraic number field. The main purpose of this thesis is to study integral discriminant matrices.

In Chapter II we generalize, slightly, a theorem of O. Taussky [11], but the main result is a characterization of the representation matrices $R_\lambda(\underline{\alpha})$ defined by the equation

$$R_\lambda(\underline{\alpha}) \cdot \underline{\alpha} = \lambda \underline{\alpha} \quad (\text{for } \lambda \in K),$$

where $\underline{\alpha}$ denotes the column vector

$$\underline{\alpha} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} .$$

Specifically, we prove that, if $\alpha_1^*, \alpha_2^*, \ldots, \alpha_n^*$ is the dual basis, then $R_\lambda(\underline{\alpha}) = (S_{K|F}(\lambda \alpha_i \alpha_j^*))$. This clarifies the connection between D_λ and R_λ-matrices. This result appears in [2], but the proof given here is independent of [2].

In Chapters III through V we make additional assumptions about $K|F$. We assume that F admits a Dedekind set of spots [10, p. 42] and that the integers $\mathbb{Z}_F$ of F form a principal ideal domain. If M is any $\mathbb{Z}_F$-module of K with an n-element $\mathbb{Z}_F$-basis $\sigma_1, \sigma_2, \ldots, \sigma_n$ we define the discriminant $d_{K|F}(M)$ to be the ideal in F generated by $\det D(\underline{\sigma})$. Since $K|F$ is separable, $d_{K|F}(M) \neq (0)$. We study conditions under which $D(\underline{\sigma})$ is integral. In particular, we assume that our modules M contain $\mathbb{Z}_K$ (the integers of K). We call M <u>almost-fundamental</u> if $D(\underline{\sigma})$ is integral and M is not contained in a larger $\mathbb{Z}_F$-module which has an integral discriminant matrix (it is easy to see that this is a property which does not depend upon the basis chosen). Let $\mathcal{A}_{K|F}$ be the set of all $\mathbb{Z}_F$-modules which contain $\mathbb{Z}_K$ and have an integral discriminant matrix. We construct an ideal which is maximal with respect to belonging to $\mathcal{A}_{K|F}$ and we show that this ideal contains every other ideal in $\mathcal{A}_{K|F}$. We then discuss some special fields in which this ideal is almost-fundamental; e. g. quadratic fields, cubic fields and cyclotomic fields.

In Chapter IV we obtain necessary and sufficient conditions on $d_{K|F}(M)$ in order that M be almost-fundamental. We adopt a proof similar to the method used by G. Pall (unpublished) to study the discriminant of a fundamental quadratic form. In the theorem we prove here, the ground field F is assumed to be either the rationals or a p-adic field.

In Chapter V the results of the previous sections are applied to characterize normal extensions $K|F$ for which $\mathbb{Z}_K$ is almost-fundamental. The ground field here is assumed to be either the rationals or

a field complete with respect to a p-adic valuation. When F is the rational field, K must be either quadratic or biquadratic.

The material prerequisite to reading this thesis can be found in LeVeque [9], Artin [1] and Zariski, Samuel [14]. The treatment of the local theory is based on the concepts and notation of O'Meara [10]; and the properties of the Hilbert symbol and Hasse symbol used in Chapter IV can be found in the appendix of [2], in O'Meara [10] or B. W. Jones [8].

II. A Characterization of R_λ - matrices

Let $K|F$ be a separable algebraic extension of F of degree n. Then there is some element θ in K such that $K = F(\theta)$. If $\theta = \theta^{(1)}$, $\theta^{(2)}, \ldots, \theta^{(n)}$ are the conjugates of θ, the mapping $\theta \to \theta^{(i)}$ sends each element α into its ith conjugate $\alpha^{(i)}$. Now, if $\alpha_1, \alpha_2, \ldots, \alpha_n$ belong to K, we let $\underline{\alpha}^{(i)}$ $(i = 1, 2, \ldots, n)$ denote the column vector

$$\underline{\alpha}^{(i)} = \begin{pmatrix} \alpha_1^{(i)} \\ \alpha_2^{(i)} \\ \vdots \\ \alpha_n^{(i)} \end{pmatrix},$$

and we let $\underline{\alpha}^{(1)} = \underline{\alpha}$. The $n \times n$ matrix whose ith column is $\underline{\alpha}^{(i)}$ will be denoted by $M(\underline{\alpha})$. From now on we assume that $\underline{\alpha}$ is a basis for K over F. Then $\det M(\underline{\alpha}) \neq 0$ since $K|F$ is separable. Also, if $\underline{\alpha}^*$ is the dual basis (i.e., $S_{K|F}(\alpha_i \alpha_j^*) = \delta_{ij}$), a simple calculation shows that

$$M(\underline{\alpha}^*)\, M'(\underline{\alpha}) = I$$

where A' is the transpose of the matrix A, and I is the identity matrix.

In this chapter we are interested in matrices of the type defined below.

2.1 Definition. Let $\underline{\alpha}$ and $\underline{\beta}$ be two bases for $K|F$. For each $\lambda \in K$ we set $T_\lambda(\underline{\alpha}, \underline{\beta}) = (S_{K|F}(\lambda \alpha_i \beta_j))$, and we let $\mathcal{T}(\underline{\alpha}, \underline{\beta})$ be the set of all of these matrices.

These matrices are F-matrices, and it is clear that $\mathcal{T}(\underline{\alpha}, \underline{\beta})$ can be regarded as a vector space of dimension n over F since each $T_\lambda(\underline{\alpha}, \underline{\beta})$ can be uniquely expressed as an F-linear combination of the matrices T_{α_1}, T_{α_2}, ..., T_{α_n}. In the special case where $\underline{\beta} = \underline{\alpha}$, we obtain the $D_\lambda(\underline{\alpha})$ matrices. We note that

$$D_\lambda(\underline{\alpha}) = M(\underline{\alpha})\, J(\lambda)\, M'(\underline{\alpha}),$$

where $J(\lambda) = \operatorname{diag}\left[\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(n)}\right]$. This result appears in a paper of O. Taussky [11].

The purpose of this chapter is to develop the connection between the D_λ-matrices and the R_λ-matrices, and we begin with the following lemma.

2.2 Lemma. For each $\lambda \in K$, $D_\lambda(\underline{\alpha}) = R_\lambda(\underline{\alpha})\, D(\underline{\alpha})$.

Proof: Let $S = (s_{ij})(s_{ij} \in F)$ be the matrix, relative to $\underline{\alpha}^*$, of the linear transformation of K determined by $\alpha_i^* \to \lambda\alpha_i$ $(i = 1, 2, \ldots, n)$. Then

$$\lambda\alpha_i = \sum_k s_{ik}\alpha_k^*,$$

and so

$$\lambda\alpha_i\alpha_j = \sum_k s_{ik}\alpha_k^*\alpha_j .$$

By taking traces in the last expression, we obtain $s_{ij} = S_{K|F}(\lambda\alpha_i\alpha_j)$. Therefore we have

$$D_\lambda(\underline{\alpha}) \cdot \underline{\alpha}^* = \lambda \cdot \underline{\alpha} .$$

When $\lambda = 1$, this becomes

$$D(\underline{\alpha}) \cdot \underline{\alpha}^* = \underline{\alpha}$$

hence, in general, we obtain

$$D_\lambda(\underline{\alpha}) \cdot \underline{\alpha}^* = R_\lambda(\underline{\alpha})\, D(\underline{\alpha}) \cdot \underline{\alpha}^*$$

and the proof is complete.

As a consequence of 2.2 we have the next corollary.

2.3 Corollary. $R_\lambda'(\underline{\alpha}) = D_\mu^{-1}(\underline{\alpha})\, R_\lambda(\underline{\alpha})\, D_\mu(\underline{\alpha})$ for each pair $\lambda,\mu \in K$.

Proof: Let $\lambda,\mu \in K$, and set $\rho = \lambda\mu$. Then

$$D_\rho(\underline{\alpha}) = R_{\lambda\mu}(\underline{\alpha})\, D_\mu(\underline{\alpha}) = R_\lambda(\underline{\alpha})\, D_\mu(\underline{\alpha}).$$

Now take the transpose of both sides to obtain

$$D_\mu(\underline{\alpha})\, R_\lambda'(\underline{\alpha}) = R_\lambda(\underline{\alpha})\, D_\mu(\underline{\alpha}).$$

Multiply both sides of the last expression by $D_\mu^{-1}(\underline{\alpha})$ to complete the proof.

O. Taussky [11] proved that if F is the rational field every matrix S which satisfies the hypotheses of theorem 2.4 below must be of the form $S = D_\lambda(\underline{\alpha})$, for some $\lambda \in K$. In 2.5 we prove a converse for the more general setting.

2.4 Theorem. Let A be an integral matrix with characteristic polynomial $f(x)$ which is irreducible over the rationals Q. Let θ be a zero of $f(x)$. Then a Q-matrix S satisfies

$$A' = S^{-1} A S$$

if and only if $S = D_\lambda(\underline{\alpha})$ for some $\lambda \in K$, where $\underline{\alpha}$ is an integral basis for some ideal contained in $\mathbb{Z}_Q[\theta]$, the ring of polynomials in θ with rational integral coefficients.

Proof: In [11] it was shown that $\underline{\alpha}$ could be chosen to be a characteristic vector of A, and so $A\underline{\alpha} = \theta \cdot \underline{\alpha}$. Hence $A = R_\theta(\underline{\alpha})$. The proof follows from the remark preceding the statement of 2.4, and from 2.3.

The converse to 2.4 can be proved in a more general setting:

2.5 Lemma. Let $A = (a_{ij})$ be an F-matrix such that

$$A' = D_\mu^{-1}(\underline{\alpha})\, A D_\mu(\underline{\alpha})$$

holds for all $\mu \in K$. Then there exists a $\lambda \in K$ such that $A = R_\lambda(\underline{\alpha})$.

Proof: The hypothesis is equivalent to the condition that $AD_\mu(\underline{\alpha})$ be symmetric for each $\mu \in K$.

Now let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be determined by the equation

$$A \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \lambda_1\alpha_1 \\ \lambda_2\alpha_2 \\ \vdots \\ \lambda_n\alpha_n \end{pmatrix}$$

We must show that $\lambda_1 = \lambda_2 = \ldots = \lambda_n$. To do this we set $AD_\mu(\underline{\alpha}) = (C_{ij}^{(\mu)})$, where

$$\begin{aligned} C_{ij}^{(\mu)} &= \sum_k a_{ik} S_{K|F}(\mu \alpha_k \alpha_j) \\ &= S_{K|F}(\mu \alpha_j \sum_k a_{ik}\alpha_k) \\ &= S_{K|F}(\mu \alpha_j \alpha_i \lambda_i). \end{aligned}$$

Now, we are assuming that $C_{ij}^{(\mu)} = C_{ji}^{(\mu)}$ for all i, j and all $\mu \in K$ and therefore we obtain

$$S_{K|F}(\mu\alpha_i\alpha_j(\lambda_i-\lambda_j)) = 0.$$

Since the trace is non-degenerate, $\lambda_i = \lambda_j$ and the lemma is proved.

We now consider the set $T(\underline{\alpha},\underline{\beta})$.

2.6 Lemma. $T(\underline{\alpha},\underline{\beta})$ is a field containing the F-scalar matrices if and only if there is a $\gamma \in K$ such that $M(\underline{\beta}) = M(\underline{\alpha}^*)\,J(\gamma)$.

Proof: (I) Suppose $T(\underline{\alpha},\underline{\beta})$ is a field. Choose any $\lambda,\mu \in K$, then there is a $\rho \in K$ such that $T_\lambda T_\mu = T_\rho$. But for any $\lambda \in K$ we have

$$T_\lambda(\underline{\alpha},\underline{\beta}) = M(\underline{\alpha})\,J(\lambda)\,M'(\underline{\beta})$$

and so

$$T_\lambda T_\mu = M(\underline{\alpha})\,J(\lambda)\,M'(\underline{\beta})\,M(\underline{\alpha})\,J(\mu)\,M'(\underline{\beta}) = M(\underline{\alpha})\,J(\rho)\,M'(\underline{\beta}).$$

It follows that $M'(\underline{\beta})\,M(\underline{\alpha}) = J(\gamma)$, where $\gamma = \rho/\lambda\mu$. Since

$$M(\underline{\alpha}^*)\,M(\underline{\alpha}) = I\ ,$$

we obtain

$$M(\underline{\beta}) = M(\underline{\alpha}^*)\,J(\gamma).$$

(II) Suppose that the last equation holds for some $\gamma \in K$; then $M'(\underline{\beta})\,M(\underline{\alpha}) = J(\gamma)$. Let $\lambda,\mu \in K$, then

$$T_\lambda T_\mu = M(\underline{\alpha})\,J(\lambda\gamma\mu)\,M'(\underline{\beta}).$$

Hence $T(\underline{\alpha},\underline{\beta})$ is closed under multiplication, and $T_\lambda T_\mu = T_\mu T_\lambda$. Moreover, each T_λ has an inverse in $T(\underline{\alpha},\underline{\beta})$. For we let $\mu = 1/\gamma^2\lambda$, and then

$$T_\lambda T_\mu = M(\underline{\alpha})\, J(\gamma^{-1})\, M'(\underline{\beta})$$
$$= M(\underline{\alpha})\, M^{-1}(\underline{\alpha}) \left[M'(\underline{\beta})\right]^{-1} M'(\underline{\beta})$$
$$= I_n.$$

In view of the remark following 2.1, the proof is complete

The next theorem is the principal result of this chapter.

2.7 Theorem. Let $\underline{\alpha}$ be a basis for $K|F$ and let $\underline{\alpha}^*$ be the dual basis. If $\underline{\beta}$ is any basis of $K|F$, then $T(\underline{\alpha}, \underline{\beta})$ coincides with the set of all $R_\lambda(\underline{\alpha})$ matrices if and only if there is a $\gamma \in K$ such that $\underline{\beta} = \gamma \underline{\alpha}^*$. Moreover, $R_\lambda(\underline{\alpha}) = (S_{K|F}(\lambda \alpha_i \alpha_j^*))$.

Proof: In view of 2.6 it is sufficient to show that if $T(\underline{\alpha}, \underline{\beta})$ is a field then it coincides with the set of $R_\lambda(\underline{\alpha})$ matrices; and because of 2.5 it is sufficient to show that for any $\mu \in K$,

$$T'_\lambda(\underline{\alpha}, \underline{\beta}) = D_\mu^{-1}(\underline{\alpha})\, T_\lambda(\underline{\alpha}, \underline{\beta})\, D_\mu(\underline{\alpha});$$

for then $T(\underline{\alpha}, \underline{\beta})$ is contained in the set of $R_\lambda(\underline{\alpha})$ matrices, and since $T(\underline{\alpha}, \underline{\beta})$ is a vector space of dimension n over F, the two sets must coincide. We therefore assume that $T(\underline{\alpha}, \underline{\beta})$ is a field; and then

$$M(\underline{\beta}) = M(\underline{\alpha}^*)\, J(\gamma)$$

for some $\gamma \in K$. We have

$$D_\mu^{-1}(\underline{\alpha})\, T_\lambda(\underline{\alpha}, \underline{\beta})\, D_\mu(\underline{\alpha}) = \left[M'(\underline{\alpha})\right]^{-1} \left[J(\mu)\right]^{-1} \left[M(\underline{\alpha})\right]^{-1} M(\underline{\alpha}) J(\lambda) M'(\underline{\beta}) M(\underline{\alpha}) J(\mu) M'(\underline{\alpha}) =$$
$$\left[M'(\underline{\alpha})\right]^{-1} J(\gamma\lambda)\, M'(\underline{\alpha}).$$

On the other hand,

$$T'_\lambda(\underline{\alpha},\underline{\beta}) = M(\underline{\beta})\, J(\lambda)\, M'(\underline{\alpha})$$

$$= \left[M'(\underline{\alpha})\right]^{-1} J(\gamma\lambda)\, M'(\underline{\alpha}).$$

This establishes the first part of the theorem.

To prove the last assertion of 2.7, we take $\underline{\beta} = \underline{\alpha}^*$. Then

$$T_\lambda(\underline{\alpha},\underline{\alpha}^*)\, D(\underline{\alpha}) = M(\underline{\alpha})\, J(\lambda)\, M'(\underline{\alpha}^*)\, M(\underline{\alpha})\, M'(\underline{\alpha})$$

$$= M(\underline{\alpha})\, J(\lambda)\, M'(\underline{\alpha})$$

$$= D_\lambda(\underline{\alpha}).$$

By 2.2 we obtain $T_\lambda(\underline{\alpha},\underline{\alpha}^*) = R_\lambda(\underline{\alpha})$.

According to this theorem both the D_λ-matrices and the R_λ-matrices can be obtained from the T_λ-matrices by taking $\underline{\beta} = \underline{\alpha}$ and $\underline{\beta} = \underline{\alpha}^*$, respectively. We can prove the following rather interesting corollary.

2.8 Corollary [1]. *Let $\underline{\alpha}$ be a field basis for $K|F$ and let $\underline{\alpha}^*$ be the dual basis. Then $\sum \alpha_i\alpha_i^* = 1$.*

Proof: For each $\lambda \in K$, we have $R_\lambda(\underline{\alpha}) = (S_{K|F}(\alpha_i\alpha_j^*\lambda))$. Hence we see that

$$S_{K|F}(\lambda) = \sum_i S_{K|F}(\alpha_i\alpha_i^*\lambda)$$

$$= S_{K|F}(\lambda \textstyle\sum_i \alpha_i\alpha_i^*).$$

Therefore $$S_{K|F}(\lambda(1 - \textstyle\sum \alpha_i\alpha_i^*)) = 0$$

for all $\lambda \in K$. The corollary follows since the trace is non-degenerate.

---

[1] This follows directly from the equation $M(\underline{\alpha}^*)\, M'(\underline{\alpha}) = I$.

III. Almost-Fundamental Modules

1. Introduction and Definitions. We shall now assume, in addition to the separability of $K|F$, that F admits a Dedekind set of spots [10, p.42], and we let $\mathfrak{S}$ denote the set of all extensions of spots on F to K. We also assume that the ring of integers $\mathbb{Z}_F$ of F is a principal ideal domain, in which case $\mathbb{Z}_K$ has an n-element $\mathbb{Z}_F$-basis [14,p.265]. The discriminant of the field $K|F$ is the discriminant of $\mathbb{Z}_K$; and we write, for short, $d_{K|F} = d_{K|F}(\mathbb{Z}_K)$. The following lemma will be used repeatedly:

3.1 Lemma. If $\mathfrak{o}$ is any ideal in $K|F$, then

$$d_{K|F}(\mathfrak{o}) = N^2_{K|F}(\mathfrak{o}) \cdot d_{K|F},$$

where $N_{K|F}(\mathfrak{o})$ is the norm of $\mathfrak{o}$.

Proof: [1, p. 133].

In the remaining chapters we will study $\mathbb{Z}_F$-modules which have an integral discriminant matrix; in particular we will be interested in modules which are maximal with respect to this property. Let M be a module with basis $\underline{\sigma}$, then with M we can associate a quadratic form, which may be written as follows:

$$f(x) = \sum_{i,j} a_{ij} x_i x_j, \quad a_{ij} = a_{ji},$$

where $a_{ij} = S_{K|F}(\sigma_i \sigma_j)$. The discriminant matrix is integral if and only if each a_{ij} is integral. G. Pall has called a quadratic form

fundamental if its coefficients are integral and it cannot be obtained from another integral form of smaller determinant by an integral transformation. Our condition that the a_{ij} be integral is stronger than requiring $f(x)$ to have integral coefficients; however, in any field for which 2 is a unit the two conditions are identical. We are thus led to make the following definition.

3.2 Definition. Let M be a $\mathbb{Z}_F$-module with an n-element $\mathbb{Z}_F$-basis σ. We call M almost fundamental if $D(\sigma)$ is integral, and M is not properly contained in any $\mathbb{Z}_F$-module with this property.

We will generally assume that M contains $\mathbb{Z}_K$ and so we define the set $\mathcal{A}_{K|F}$ below.

3.3 Definition. Let $\mathcal{A}_{K|F}$ be the set of all $\mathbb{Z}_F$-modules M which satisfy the two conditions:

(a) $M \supseteq \mathbb{Z}_K$

(b) If $\alpha, \beta \in M$, then $S_{K|F}(\alpha\beta) \in \mathbb{Z}$.

3.4 Lemma. Let $\mathfrak{d}_{K|F}$ be the different of $K|F$. Then

$$\mathfrak{d}_{K|F}^{-1} \supseteq M \supseteq \mathbb{Z}_K$$

for every $M \in \mathcal{A}_{K|F}$. Moreover, $\mathfrak{d}_{K|F}^{-1} \in \mathcal{A}_{K|F}$ if and only if $d_{K|F} = \mathbb{Z}_F$.

Proof: Since $\mathfrak{d}_{K|F}^{-1}$ is defined by

$$\mathfrak{d}_{K|F}^{-1} = \{x \in K \mid S_{K|F}(x\mathbb{Z}_K) \subseteq \mathbb{Z}_F\}$$

the first part of the lemma is obvious.

Now let $\underline{\omega}$ be an integral basis for $\mathbb{Z}_K$, then the dual basis $\underline{\omega}^*$ is a $\mathbb{Z}_K$-basis for $\mathfrak{d}_{K|F}^{-1}$. Hence $\mathfrak{d}_{K|F}^{-1} \in \mathcal{A}_{K|F}$ if and only if $D(\underline{\omega}^*)$ is integral. Now,

$$\begin{aligned} D(\underline{\omega}^*) &= M(\underline{\omega}^*)\, M'(\underline{\omega}^*) \\ &= [M'(\underline{\omega})]^{-1} [M(\underline{\omega})]^{-1} \\ &= D^{-1}(\underline{\omega}). \end{aligned}$$

Therefore $\mathfrak{d}_{K|F}^{-1} \in \mathcal{A}_{K|F}$ if and only if $d_{K|F} = \mathbb{Z}_F$.

Since $\mathbb{Z}_F$ is a principal ideal domain, and $\mathbb{Z}_K$ has an n-element basis, it follows that every module in $\mathcal{A}_{K|F}$ has an n-element $\mathbb{Z}_F$-basis (and so condition (b) in 3.3 is equivalent to requiring that M have an integral discriminant matrix). Suppose now that

$$M_1 \subseteq M_2 \subseteq \cdots$$

is a chain of elements from $\mathcal{A}_{K|F}$, and let

$$M^* = \left\{ \sum_{\text{finite}} m_i \;\middle|\; m_i \in M_i \right\}$$

Then $M^* \in \mathcal{A}_{K|F}$ for (a) is obvious, and if $\alpha, \beta \in M^*$ there is some k for which $\alpha, \beta \in M_k$; hence (b) is satisfied. By Zorn's lemma, we see that $\mathcal{A}_{K|F}$ contains almost-fundamental modules. In the remainder of Chapter III we study modules belonging to $\mathcal{A}_{K|F}$.

2. The Largest Ideal in $\mathcal{A}_{K|F}$. We would like to say something about the almost-fundamental modules in $\mathcal{A}_{K|F}$. This seems to be difficult, but we can say something about the ideal in $\mathcal{A}_{K|F}$. In this section, therefore, we study the ideal which are maximal with respect to the

property of belonging to $\mathcal{A}_{K|F}$.

3.5 Lemma[2]. Let $M \in \mathcal{A}_{K|F}$. If M is an ideal then $M^2 \subseteq \mathfrak{d}^{-1}_{K|F}$. If M is almost-fundamental it is an ideal if and only if $M^2 \subseteq \mathfrak{d}^{-1}_{K|F}$.

Proof: (I) Suppose M is an ideal, and let $\alpha, \beta \in M$. Then $\beta M \subseteq M$, and so $S_{K|F}(\alpha\beta\mathbb{Z}_K) \subseteq \mathbb{Z}_F$. Therefore $\alpha\beta \in \mathfrak{d}^{-1}_{K|F}$ and $M^2 \subseteq \mathfrak{d}^{-1}_{K|F}$.

(II) Suppose M is almost-fundamental, and suppose $M^2 \subseteq \mathfrak{d}^{-1}_{K|F}$. Let $\alpha \in M$ and consider the $\mathbb{Z}_F$-module $\alpha\mathbb{Z}_K + M = M_1$. Clearly $M_1 \supseteq \mathbb{Z}_K$. Let $\alpha x + m_1$ and $\alpha y + m_2$ $(x, y \in \mathbb{Z}_K ; m_1, m_2 \in M)$ be any two elements of M_1, then

$$(\alpha x + m_1)(\alpha y + m_2) = \alpha^2 xy + \alpha m_1 y + m_1 m_2 + \alpha m_2 x$$

and

$$S_{K|F}(\alpha^2 xy) + S_{K|F}(\alpha m_1 y) + S_{K|F}(m_1 m_2) + S_{K|F}(\alpha m_2 x) \in \mathbb{Z}_F .$$

So $M_1 \in \mathcal{A}_{K|F}$. But M is almost-fundamental and hence $M_1 = M$, which implies that $\alpha\mathbb{Z}_K \subseteq M$. Therefore M is an ideal.

2a. The Local Case. We now consider the case where F is complete with respect to a single spot.

3.6 Theorem. Let K|F be an extension of the complete field F and let $\mathfrak{P}$ denote the prime ideal in K; also, let $\mathfrak{d}_{K|F} = \mathfrak{P}^{\delta}$. Then the ideal $M_{\mathfrak{P}} = \mathfrak{P}^{-[\delta/2]}$ belongs to $\mathcal{A}_{K|F}$. Here $[x]$ denotes the greatest

---

[2] The main theorems of this chapter can be proved directly from lemma 3.5. However, we wish also to develop the connection between the local and global theory; therefore no attempt has been made here to give the shortest possible proofs.

integer in x.

Proof: Since there is only one prime ideal $\mathfrak{P}$, and every ideal of K is a power of the prime ideal, it is sufficient to show that $M_{\mathfrak{P}} = \mathfrak{P}^{-[\delta/2]}$ is the largest ideal in $\mathfrak{A}_{K|F}$.

Let Π be a prime element and let $n = ef$, where e is the ramification index and f is the inertial index. Then there are units $\omega_1, \omega_2, \ldots, \omega_f$ in K such that

$$\mathbb{Z}_K = \prod_{\substack{1 \le i \le f \\ 1 \le j \le e}} \mathbb{Z}_F \, \omega_i \Pi^j,$$

[1, p. 84].

Now clearly $M_{\mathfrak{P}} \supseteq \mathbb{Z}_K$. So suppose $\alpha, \beta \in M_{\mathfrak{P}}$ and write

$$\alpha = \frac{\alpha_1}{\Pi^{k_1}}, \quad \beta = \frac{\beta_1}{\Pi^{k_2}},$$

where $\alpha_1, \beta_1 \in \mathbb{Z}_K$, and $k_1 + k_2 \le 2[\delta/2]$. Let

$$\alpha_1 \beta_1 = \sum a_{ij} \omega_i \Pi^j; \quad a_{ij} \in \mathbb{Z}_F,$$

so that

$$\alpha\beta = \sum \frac{a_{ij} \omega_i}{\Pi^{(k_1 + k_2 - j)}}.$$

Since $k_1 + k_2 - j \le \delta - j$, $\alpha\beta \in \mathfrak{d}^{-1}_{K|F}$; and so $S_{K|F}(\alpha\beta) \in \mathbb{Z}_F$. Therefore $M_{\mathfrak{P}} \in \mathfrak{A}_{K|F}$.

Suppose $\mathfrak{P}^s$ is the largest ideal in $\mathfrak{A}_{K|F}$; then $s \ge [\delta/2]$. But from 3.5, $2s \le \delta$, and so $s = [\delta/2]$.

The proof is complete.

3.7 Corollary. The discriminant of the ideal $M_{\mathcal{B}}$ of 3.6 is

$$d_{K|F}(M_{\mathcal{B}}) = (N_{K|F}(\mathcal{B}))^{(\delta - 2[\delta/2])}.$$

Proof: The discriminant of $K|F$ is $(N_{K|F}(\mathcal{B}))^{\delta}$. The corollary follows by applying 2.1.

Now suppose that T is the largest unramified extension of F contained in K, so that $f = [T:F]$ and $e = [K:T]$.

3.8 Lemma. If M is a $\mathcal{Z}_T$-module contained in $\mathcal{A}_{K|T}$, then $M \in \mathcal{A}_{K|F}$.

Proof: Clearly M is a $\mathcal{Z}_T$-module containing $\mathcal{Z}_K$, and so it is sufficient to verify that (b) of 3.3 is satisfied. If $\alpha, \beta \in M$ then

$$S_{K|F}(\alpha\beta) = S_{T|F}(S_{K|T}(\alpha\beta)) \in \mathcal{Z}_F .$$

3.9 Lemma. If M is a $\mathcal{Z}_T$-module and $M \in \mathcal{A}_{K|F}$, then $M \in \mathcal{A}_{K|T}$.

Proof: We have $M \supseteq \mathcal{Z}_K \supseteq \mathcal{Z}_T$. Now suppose $\alpha, \beta \in M$. Since M is a $\mathcal{Z}_T$-module, $\beta\mathcal{Z}_T \subseteq M$, and so $S_{K|F}(\alpha\beta\mathcal{Z}_T) \subseteq \mathcal{Z}_F$. But

$$\begin{aligned} S_{K|F}(\alpha\beta\mathcal{Z}_T) &= S_{T|F}(S_{K|T}(\alpha\beta\mathcal{Z}_T)) \\ &= S_{T|F}(S_{K|T}(\alpha\beta)\mathcal{Z}_T) . \end{aligned}$$

Therefore, since $T|F$ is unramified, $S_{K|T}(\alpha\beta)$ belongs to $\mathcal{D}_{T|F}^{-1} = \mathcal{Z}_T$. Hence M satisfies (a) and (b) of 3.3.

We now need the concept of the complementary module

3.10 Definition. If M is a $\mathcal{Z}_F$-module, the complementary module $C(M)$ is defined to be the following set:

$$\mathcal{C}(M) = \{ x \in K \mid S_{K|F}(xM) \subseteq \mathbb{Z}_F \} .$$

3.10 Lemma. Let M_1 and M_2 be two $\mathbb{Z}_F$-modules then the following are true

(a) If M_1 has an n-element basis σ, then σ^* is a basis for $\mathcal{C}(M_1)$.

(b) If $M_1 \subseteq M_2$ then $\mathcal{C}(M_1) \supseteq \mathcal{C}(M_2)$

(c) $\mathcal{C}\mathcal{C}(M_1) = M_1$

(d) If M_1 is an ideal, then so is $\mathcal{C}(M_1)$

(e) If M_1 is an ideal, then $\mathcal{C}(M_1)M_1 = \mathfrak{d}_{K|F}^{-1}$.

Proof: See [14].

3.12 Lemma. Let M be a $\mathbb{Z}_F$-module containing $\mathbb{Z}_K$. Then $M \in \mathcal{A}_{K|F}$ if and only if $\mathcal{C}(M) \supseteq M$.

Proof: If $M \in \mathcal{A}_{K|F}$, then for each $m \in M$, $S_{K|F}(mM) \subseteq \mathbb{Z}_F$ and so $m \in \mathcal{C}(M)$. The converse is obvious.

Note that 3.10 through 3.12 hold for the general extension $K|F$. We can now prove the following theorem.

3.13 Theorem. Let $K|F$ be an extension of the complete field F, and $\mathfrak{P}$ be the prime ideal. Let T be the largest unramified extension of F contained in K; and let $\mathfrak{d}_{K|F} = \mathfrak{P}^{\delta}$, ($\delta$ is called the differential exponent of $\mathfrak{P}$ [14, p. 298]), with $M_{\mathfrak{P}}$ the ideal of 2.6. Then $M_{\mathfrak{P}}$ is the largest $\mathbb{Z}_T$-module contained in $\mathcal{A}_{K|F}$.

If 2 divides the differential exponent of $\mathfrak{P}$, then $M_{\mathfrak{P}}$ is almost-fundamental. Also if $K|F$ is unramified or fully ramified,

then $M_{\mathfrak{P}}$ is almost-fundamental.

Proof: Suppose that $M_{\mathfrak{P}}$ is properly contained in a $\mathbb{Z}_T$-module N. We show that this leads to a contradiction. By 3.9 both $M_{\mathfrak{P}}$ and N belong to $\mathcal{A}_{K|T}$. Also $K|T$ is fully ramified, and so $N_{K|T}(\mathfrak{P}) = \mathfrak{p}$, the prime ideal in T.

Now, because of (e) in 2.11, we see that

$$C(M_{\mathfrak{P}}) = \begin{cases} M_{\mathfrak{P}} & \text{if } 2 \mid \delta \\ \mathfrak{P} - [\delta/2] - 1 & \text{otherwise.} \end{cases}$$

If $N \underset{\neq}{\supset} M_{\mathfrak{P}}$, then $C(N) \underset{\neq}{\subset} C(M_{\mathfrak{P}})$, and by 3.12 we obtain

$$C(M_{\mathfrak{P}}) \underset{\neq}{\supset} C(N) \underset{\neq}{\supset} N \underset{\neq}{\supset} M_{\mathfrak{P}}.$$

If 2 divides δ this is not possible. Since this contradiction can also be obtained if N is only a $\mathbb{Z}_F$-module, the second assertion of the theorem is proved. Now suppose 2 does not divide δ. Since $C(M_{\mathfrak{P}}) \underset{\neq}{\supset} N \underset{\neq}{\supset} M_{\mathfrak{P}}$, the discriminants $d_{K|T}(C(M_{\mathfrak{P}}))$ and $d_{K|T}(M_{\mathfrak{P}})$ must differ by at least a fourth power of $\mathfrak{p}$. We use 3.1 to obtain

$$d_{K|T}(M_{\mathfrak{P}}) = \mathfrak{p}^{-2[\delta/2]} \cdot \mathfrak{p}^{\delta} = \mathfrak{p},$$

and

$$d_{K|T}(C(M_{\mathfrak{P}})) = \mathfrak{p}^{-2[\delta/2]-2} \mathfrak{p}^{\delta} = \mathfrak{p}^{-1}.$$

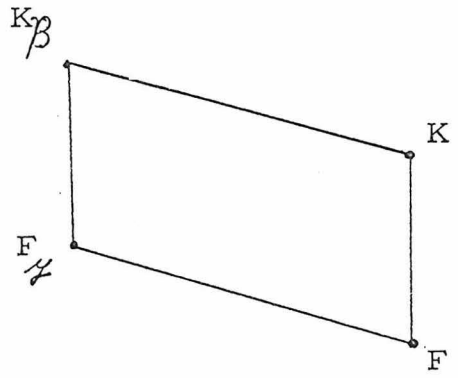
Comparing the two discriminants, we obtain a contradiction. Therefore $M_{\mathfrak{P}} = N$.

To complete the proof we notice that if $K|F$ is unramified, then

$\mathfrak{d}_{K|F}^{-1} = M_{\mathfrak{P}} = \mathbb{Z}_K$, and so $M_{\mathfrak{P}}$ is almost-fundamental. If $K|F$ is fully ramified, then $T = F$ and again $M_{\mathfrak{P}}$ is almost-fundamental.

The proof is complete.

2b. The General Case. We return to the general case. For each $\mathfrak{P} \in \mathfrak{D}$ let $K_{\mathfrak{P}}$ be the completion of K at $\mathfrak{P}$, and let $F_{\mathfrak{p}}$ denote the completion of F in $K_{\mathfrak{P}}$ so that $\mathfrak{P} | \mathfrak{p}$.



Let $\mathbb{Z}_{\mathfrak{P}}$ and $\mathbb{Z}_{\mathfrak{p}}$ denote the integers of $K_{\mathfrak{P}}$ and $F_{\mathfrak{p}}$ respectively. We will also let $\mathfrak{P}$ denote the prime ideal in $K_{\mathfrak{P}}$, and set $\tilde{\mathfrak{P}} = \mathfrak{P} \cap \mathbb{Z}_K$, the prime ideal in K determined by $\mathfrak{P}$. Now if $\mathfrak{A}$ is any ideal in K, then it can be factored uniquely into a product of prime ideals

$$\mathfrak{A} = \prod_{\mathfrak{P} \in \mathfrak{D}} \tilde{\mathfrak{P}}^{(\mathrm{ord}_{\mathfrak{P}} \mathfrak{A})}$$

where $\mathrm{ord}_{\mathfrak{P}} \mathfrak{A}$ is the exponent of the highest power of $\mathfrak{P}$ which divides $\mathfrak{A}$. Finally, if U is any ideal in $K_{\mathfrak{P}}$, we let $\tilde{U} = \tilde{\mathfrak{P}}^{(\mathrm{ord}_{\mathfrak{P}} U)}$.

The method of this section is to consider $K|F$ at each of its completions $K_{\mathfrak{P}}|F_{\mathfrak{p}}$, and apply the results of 2a to $K_{\mathfrak{P}}|F_{\mathfrak{p}}$. Hence we must now establish the connection between the general case and the local case.

3.14 Definition. If N is a Z_F-module in K, we let $N_\beta = N Z_\mathfrak{y}$. (Then N_β is a Z-module in K_β.)

We will need the following lemma.

3.15 Lemma. $Z_\beta = Z_K Z_\mathfrak{y}$.

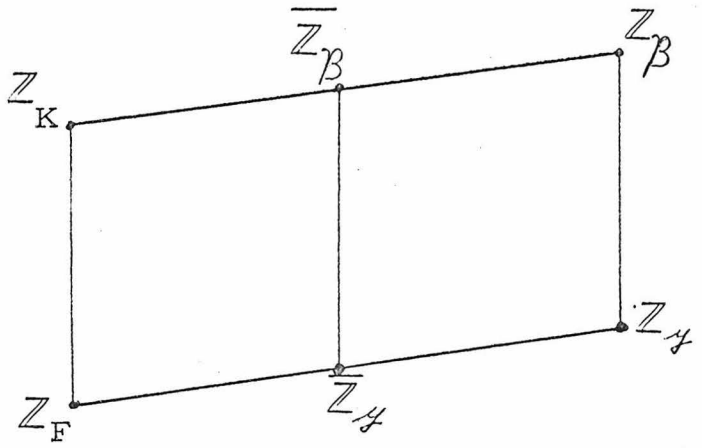
Proof: Let $\overline{Z}_\beta$ be the quotient ring

$$\overline{Z}_\beta = \{a/b \mid a, b \in Z_K;\ b \notin \tilde{\beta}\},$$

and let $\overline{Z}_\mathfrak{y}$ be the quotient ring

$$\overline{Z}_\mathfrak{y} = \{a/b \mid a, b \in F;\ b \notin \tilde{\mathfrak{y}}\}.$$

The inclusion relations are diagrammed below:



Now, it is known ([3], p. 13) that $\overline{Z}_\beta = Z_K \overline{Z}_\mathfrak{y}$; and we see that

$$\overline{Z}_\beta = Z_K \overline{Z}_\mathfrak{y} \subseteq Z_K Z_\mathfrak{y} \subseteq Z_\beta .$$

Since Z_β is the closure in K_β of $\overline{Z}_\beta$, it will be sufficient to show that $Z_K Z_\mathfrak{y}$ is closed. Let $\underline{\omega}$ be an integral basis for Z_K; then

$$Z_K Z_\mathfrak{y} = \sum_i \omega_i Z_\mathfrak{y} .$$

Consider Z_β as a topological group under addition. Then $Z_\mathfrak{y}$ is a closed, compact subgroup of Z_β, and so is $\omega_i Z_\mathfrak{y}$. Therefore,

$\mathcal{Z}_K\ \mathcal{Z}_{\mathcal{Y}}$ is closed ([7], p. 48).

3.16 Lemma. Let $\mathcal{O}$ be an ideal in K. Then for each $\beta \in \mathcal{D}$, $\mathcal{O}_\beta$ is an ideal in K_β; and

$$\mathcal{O} = \prod_{\beta \in \mathcal{D}} \tilde{\mathcal{O}}_\beta .$$

Proof: It is clear that $\mathcal{O}_\beta$ is an ideal since

$$\mathcal{O}_\beta\ \mathcal{Z}_\beta = \mathcal{O}\ \mathcal{Z}_{\mathcal{Y}}\ \mathcal{Z}_K\ \mathcal{Z}_{\mathcal{Y}} \subseteq \mathcal{O}_\beta$$

In order to complete the proof, we must show that $\mathcal{O}_\beta = \beta^{(\mathrm{ord}_\beta \mathcal{O})}$. Now

$$\mathcal{O}_\beta \subseteq \beta^{(\mathrm{ord}_\beta \mathcal{O})} = \{x \in K_\beta \mid \mathrm{ord}_\beta\, x \geq \mathrm{ord}_\beta\, \mathcal{O}\} ;$$

but $\mathcal{O}_\beta$ contains an element α with $\mathrm{ord}_\beta\, \alpha = \mathrm{ord}_\beta\, \mathcal{O}$, and $\mathcal{O}_\beta$ is an ideal, so we must have $\mathcal{O}_\beta = \beta^{(\mathrm{ord}_\beta \mathcal{O})}$.

We now study the connection between $A_{K|F}$ and $A_{K_\beta|F_{\mathcal{Y}}}$.

3.17 Lemma. Let $\mathcal{O}$ be an ideal in K, and suppose that $\mathcal{O} \in A_{K|F}$. Then $\mathcal{O}_\beta \in A_{K_\beta|F_{\mathcal{Y}}}$.

Proof: First,

$$\mathcal{O}_\beta = \mathcal{O}\ \mathcal{Z}_\beta \supseteq \mathcal{Z}_K\ \mathcal{Z}_{\mathcal{Y}} = \mathcal{Z}_\beta$$

Now let $\alpha, \beta \in \mathcal{O}_\beta$; we wish to show that (write $S_{\beta|\mathcal{Y}}$ for $S_{K_\beta|F_{\mathcal{Y}}}$) $S_{\beta|\mathcal{Y}}(\alpha, \beta) \in \mathcal{Z}_{\mathcal{Y}}$. Since any element of $\mathcal{O}_\beta$ is a finite sum of terms of the form uv ($u \in \mathcal{O}$, $v \in \mathcal{Z}_{\mathcal{Y}}$), it is clearly sufficient to assume $\alpha = \alpha_1\gamma$, $\beta = \beta_1\delta$, where $\alpha_1, \beta_1 \in \mathcal{O}$ and $\gamma, \delta \in \mathcal{Z}_{\mathcal{Y}}$. Then

$$S_{\beta|\mathcal{Y}}(\alpha\beta) = \gamma\delta S_{\beta|\mathcal{Y}}(\alpha_1\beta_1) .$$

We will be finished if we can show that $S_{\mathfrak{P}|\mathfrak{p}}(\alpha_1\beta_1) \in \mathfrak{Z}_{\mathfrak{p}}$. Let U be the principal ideal generated by $\alpha_1\beta_1$ in K, and let

$$U = \prod_{\mathfrak{P}' \in \mathfrak{D}} \tilde{U}_{\mathfrak{P}'} .$$

It is known ([6], p. 430) that $S_{K|F}(U)$ is integral if and only if $S_{\mathfrak{P}'|\mathfrak{p}'}(U_{\mathfrak{P}'})$ is integral for all $\mathfrak{P}' \in \mathfrak{D}$. But $S_{K|F}(\alpha_1\beta_1)$ is integral, and so $S_{\mathfrak{P}|\mathfrak{p}}(\alpha_1\beta_1)$ must be integral also.

This completes the proof of the lemma.

We can now prove one of the main theorems of this chapter.

3.18 Theorem. For each $\mathfrak{P} \in \mathfrak{D}$, let $M_{\mathfrak{P}}$ be the ideal determined in 3.6. The set of ideals in $\mathcal{A}_{K|F}$ has a unique maximal element

$$M = \prod_{\mathfrak{P} \in \mathfrak{D}} \tilde{M}_{\mathfrak{P}} .$$

Proof: From 3.4 and the fact that F has only finitely many ramified primes, we see that $M_{\mathfrak{P}} = \mathfrak{Z}_{\mathfrak{P}}$ for almost all $\mathfrak{P} \in \mathfrak{D}$. Hence, M is an ideal in K. Moreover, since $M_{\mathfrak{P}} \supseteq \mathfrak{Z}_{\mathfrak{P}}$ for all $\mathfrak{P} \in \mathfrak{D}$, we see that $M \supseteq \mathfrak{Z}_K$. Now

$$\mathfrak{d}_{K|F} = \prod_{\mathfrak{P} \in \mathfrak{D}} \tilde{\mathfrak{d}}_{\mathfrak{P}|\mathfrak{p}} ,$$

and $M^2 \subseteq \mathfrak{d}^{-1}_{\mathfrak{P}|\mathfrak{p}}$ (by 3.5). So $M^2 \subseteq \mathfrak{d}^{-1}_{K|F}$, and, again by 3.5, $M \in \mathcal{A}_{K|F}$.

Suppose that $\mathfrak{A}$ is an ideal in $\mathcal{A}_{K|F}$. Then, by 3.16, at each $\mathfrak{P} \in \mathfrak{D}$, $\mathfrak{A}_{\mathfrak{P}}$ is an ideal, and by 3.17 $\mathfrak{A}_{\mathfrak{P}} \in \mathcal{A}_{K_{\mathfrak{P}}|F_{\mathfrak{p}}}$; hence, $\mathfrak{A}_{\mathfrak{P}} \subseteq M_{\mathfrak{P}}$ because of 3.6. Therefore, $\mathfrak{A} \subseteq M$, and the proof is complete. We have, in fact, proved that M contains every ideal belonging to $\mathcal{A}_{K|F}$.

The previous theorem generalizes 3.6 , and the next theorem is a generalization of 3.7. But before stating the theorem, we introduce some notation. For each $\mathfrak{P} \in \mathfrak{D}$ let $f(\mathfrak{P}\,|\,\mathfrak{p})$ be the inertial index of $K_{\mathfrak{P}}\,|\,F_{\mathfrak{p}}$, let $e(\mathfrak{P}\,|\,\mathfrak{p})$ be the ramification index of $K_{\mathfrak{P}}\,|\,F_{\mathfrak{p}}$, and let $\delta(\mathfrak{P}\,|\,\mathfrak{p})$ be the differential exponent of $\mathfrak{P}$ (see 3.13). Let $\mu(\mathfrak{P}\,|\,\mathfrak{p})$ be defined by

$$\mu(\mathfrak{P}\,|\,\mathfrak{p}) = \begin{cases} 0 & \text{if } 2 \mid \delta(\mathfrak{P}\,|\,\mathfrak{p}) \\ 1 & \text{otherwise.} \end{cases}$$

3.19 Theorem. Let M be the ideal determined in 3.18. Then

$$d_{K|F}(M) = \prod_{\mathfrak{p} \mid d_{K|F}} d_{\mathfrak{p}}^{\,},$$

where

$$d_{\mathfrak{p}} = \mathfrak{p}^{\sum_{\mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}|\mathfrak{p})\mu(\mathfrak{P}|\mathfrak{p})}.$$

Proof: By 3.1 we have

$$d_{K|F}(M) = N_{K|F}^{2}(M) \cdot d_{K|F}\,,$$

and

$$N_{K|F}(M) = \prod_{\mathfrak{P} \in \mathfrak{D}} N_{K|F}(M_{\mathfrak{P}}) = \prod_{\mathfrak{P} \in \mathfrak{D}} N_{K_{\mathfrak{P}}|F_{\mathfrak{p}}}(M_{\mathfrak{P}})$$

$$= \prod_{\mathfrak{p} \mid d_{K|F}} \prod_{\mathfrak{P}|\mathfrak{p}} N_{K_{\mathfrak{P}}|F_{\mathfrak{p}}}(M_{\mathfrak{P}})\,.$$

The last expression is obtained since $M_{\mathfrak{P}} = \mathbb{Z}_{\mathfrak{P}}$ if $\mathfrak{p} \nmid d_{K|F}$.

Also,

$$d_{K|F} = \prod_{\mathfrak{p} \mid d_{K|F}} \prod_{\mathfrak{P}|\mathfrak{p}} d_{K_{\mathfrak{P}}|F_{\mathfrak{p}}}\,,$$

([6], p. 429). Hence, we obtain

$$d_{K|F}(M) = \prod_{\mathfrak{x}|d_{K|F}} \prod_{\mathfrak{B}|\mathfrak{x}} N^2_{K_{\mathfrak{B}}|F_{\mathfrak{x}}}(M_{\mathfrak{B}}) \cdot d_{K_{\mathfrak{B}}|F_{\mathfrak{x}}}$$

$$= \prod_{\mathfrak{x}|d_{K|F}} \prod_{\mathfrak{B}|\mathfrak{x}} \mathfrak{x}^{f(\mathfrak{B}|\mathfrak{x})\mu(\mathfrak{B}|\mathfrak{x})}$$

$$= \prod_{\mathfrak{x}|d_{K|F}} d_{\mathfrak{x}} ,$$

by applying 3.1 and 3.7 .

We will use this theorem in the next section.

3. Special Fields. We shall consider the following question: when is the ideal of 3.18 almost-fundamental? As we show in chapter IV, it is not always almost-fundamental; but it is in the special fields we investigate in this section. In theorem 3.13 , the ideal $M_{\mathfrak{B}}$ was seen to be almost-fundamental if the differential exponent is divisible by 2 , or if $K_{\mathfrak{B}}|F_{\mathfrak{x}}$ is either unramified or totally ramified. The question of whether or not $M_{\mathfrak{B}}$ is almost-fundamental in the remaining case is still open. In this section, we shall investigate quadratic, cubic, and cyclotomic number fields over the rationals, and show that in each case the ideal of 3.18 is almost-fundamental. The problem of determining for what other number fields the ideal is almost-fundamental is still open.

3a. Quadratic Fields

3.20 Theorem. Let $K = Q(\sqrt{D})$ be a quadratic extension of the rational field Q . Then there is exactly one almost-fundamental module, call it M , containing $\mathbb{Z}_K$; and

(a) If $D \equiv 1 \pmod 4$, then $M = \mathbb{Z}_K$.

(b) If $D \equiv 2 \pmod 4$, then

$$M = \mathbb{Z}_Q \oplus \frac{\sqrt{D}}{2} \mathbb{Z}_Q .$$

(c) If $D \equiv 3 \pmod 4$, then

$$M = \mathbb{Z}_Q \oplus \frac{1+\sqrt{D}}{2} \mathbb{Z}_Q .$$

In each case M is an ideal.

Proof: If $D \equiv 1 \pmod 4$, then $d_{K|Q} = D$ is square-free, and so $\mathbb{Z}_K$ is the only almost-fundamental module in $\mathcal{A}_{K|Q}$. We assume, therefore, that $D \not\equiv 1 \pmod 4$.

Let p be an odd prime and suppose $\mathfrak{P}|p$. Then, since $p \| d_{K|Q}$ or $p \nmid d_{K|Q}$, it is clear that $K_{\mathfrak{P}}|Q_p$ is unramified and so $M_{\mathfrak{P}} = \mathbb{Z}_{\mathfrak{P}}$. Now we consider the case $p = 2$, and suppose $2^r \| d_{K|Q}$. The prime 2 ramifies, and $(2) = \mathfrak{P}^2$; the local extension is fully ramified, and so the differential exponent δ is either 2 or 3 (also note that $\delta = r$). Thus,

$$M_{\mathfrak{P}} = \{x \in K_{\mathfrak{P}} \mid |x|_{\mathfrak{P}} \leq \sqrt{2}\} ,$$

where $|\ |_{\mathfrak{P}}$ is a valuation determined by $\mathfrak{P}$. Now, in view of 3.18, it is clear that

$$M = \{x \in K \mid |x|_p \leq 1 \text{ if } p \neq 2 ;\ |x|_2 \leq \sqrt{2}\} .$$

In particular, $M \neq \mathbb{Z}_K$, and it follows from this that M is almost-fundamental, since $d_{K|Q}(M)$ is obtained from $d_{K|Q}$ by dividing out the square factor.

We now determine an integral basis for M. The defining polynomial of $\sqrt{D}$ is $f(x) = x^2 - D$, and

$$\mathfrak{d}_{K|Q}^{-1} = C(\mathbb{Z}_K) = \frac{1}{f'(\sqrt{D})} \cdot \mathbb{Z}_K .$$

Therefore, $\mathfrak{d}_{K|Q}^{-1}$ has $1/2$, $\sqrt{D}/2D$ as an integral basis. Now, by 3.4, $M \subseteq \mathfrak{d}_{K|Q}^{-1}$; so if $\alpha \in M$,

$$\alpha = \frac{a'}{2} + \frac{b'}{2D}\sqrt{D} \; ; \; a', b' \in \mathbb{Z}_Q .$$

Now M is an ideal and $M \supseteq \mathbb{Z}_K$, so $2\alpha - a' = \frac{b'}{D}\sqrt{D} \in M$. Suppose that p ($p \neq 2$) is a prime divisor of D; then

$$\left| \frac{b'}{D}\sqrt{D} \right|_p = |b'|_p \sqrt{p} \; ,$$

and this is larger than 1 unless p divides b. Therefore, every odd prime divisor of D must divide b.

Case I: Suppose $D \equiv 2 \pmod 4$. Then, in view of the last remark, we can write α in the form

$$\alpha = \frac{a}{2} + \frac{b}{4}\sqrt{D} \; , \text{ with } a, b \in \mathbb{Z}_Q .$$

Now, $\left|\frac{a}{2}\right|_2 = 2|a|_2$ and $\left|\frac{b}{4}\sqrt{D}\right|_2 = 2\sqrt{2}\,|b|_2$. Thus, we must have $2|b$ and $2|a$. So

$$M \subseteq \mathbb{Z}_Q \oplus \frac{\sqrt{D}}{2} \mathbb{Z}_Q \; ;$$

but every element of the module on the right side of this expression belongs to M, and so we have equality.

Case II: Suppose $D \equiv 3 \pmod 4$. Then we can write α in the form

$$\alpha = \frac{a + b\sqrt{D}}{2} \quad ; \; a, b \in \mathbb{Z}_Q .$$

Now, $\left|\frac{a}{2}\right|_2 = 2|a|_2$ and $\left|\frac{b}{2}\sqrt{D}\right|_2 = 2|b|_2$; hence, $a \equiv b \pmod 2$, for otherwise $|\alpha|_2 > \sqrt{2}$. Therefore,

$$M \subseteq \mathbb{Z}_Q \oplus \frac{1+\sqrt{D}}{2} \mathbb{Z}_Q .$$

In order to establish equality, it is sufficient to show that $(1+\sqrt{D})/2$ belongs to M. If $p \neq 2$, then $\left|\frac{1+\sqrt{D}}{2}\right|_p \leq 1$. Suppose $p = 2$; then

$$\left|\frac{1+\sqrt{D}}{2}\right|_2 = \sqrt{\left|N\left(\frac{1+\sqrt{D}}{2}\right)\right|_2} = \sqrt{\left|\frac{1-D}{4}\right|_2} = \sqrt{2},$$

since $D \equiv 3 \pmod 4$. Therefore,

$$M = \mathbb{Z}_Q \oplus \frac{1+\sqrt{D}}{2}\,\mathbb{Z}_Q .^{3}$$

The analysis used above can be applied to any $\mathbb{Z}_Q$-module in $\mathcal{A}_{K|Q}$ to show that it must be contained in M. The proof is complete.

3b. Cubic Fields

3.21 Theorem. Let K be a cubic extension of the rationals Q. Then the ideal, M, determined by 3.18 is almost-fundamental.

Proof: By 3.19 we have

$$d_{K|Q}(M) = \prod_{p \mid d_{K|Q}} \prod_{\mathfrak{P} \mid p} d_p ,$$

where

$$d_p = p^{\sum_{\mathfrak{P} \mid p} f(\mathfrak{P}\mid p)\mu(\mathfrak{P}\mid p)} .$$

We will show that $d_{K|Q}(M)$ is square-free.

Let $p \mid d_{K|Q}$, and suppose

$$p = \prod_{\mathfrak{P} \mid p} \tilde{\mathfrak{P}}^{e_{\mathfrak{P}}}$$

is the factorization of p in $\mathbb{Z}_K$, and suppose r is the number of terms in the product. Now, at least one $e_{\mathfrak{P}} > 1$ and so $r \leq 2$. Hence, we have the following possibilities:

---

[3] These results, in the case of a quadratic field, can also be obtained without p-adic analysis.

$$p = \tilde{\mathfrak{p}}_1 \tilde{\mathfrak{p}}_2^2$$

or

$$p = \tilde{\mathfrak{p}}_1^3 .$$

Suppose $p = \tilde{\mathfrak{p}}_1 \tilde{\mathfrak{p}}_2^2$. Since $e(\mathfrak{p}_1|p) = 1$, $\mu(\mathfrak{p}_1|p) = 0$, and

$$d_p = p^{f(\mathfrak{p}_2|p)\mu(\mathfrak{p}_2|p)} .$$

Now, $f(\mathfrak{p}_2|p) = 1$, for otherwise $e(\mathfrak{p}_2|p) = 1$; hence, the exponent of d_p is at most 1. Suppose $p = \mathfrak{p}_1^3$. Then

$$d_p = p^{f(\mathfrak{p}_1|p)\mu(\mathfrak{p}_1|p)} .$$

But $f(\mathfrak{p}_1|p) \cdot e(\mathfrak{p}_1|p) = 3$, and so $f(\mathfrak{p}_1|p) = 1$; therefore, the exponent of d_p is again at most 1. The proof is complete, since this is true for every prime divisor of $d_{K|Q}$.

3c. Cyclotomic Fields

3.22 Theorem. Let K be a cyclotomic extension of Q of degree p-1 (where p is an odd prime). Then the ideal, M, determined by 3.18 is principal and almost-fundamental.

Proof: The field discriminant is given by

$$d_{K|Q} = (-1)^{\frac{p-1}{2}} \cdot p^{p-2} .$$

Hence, if q is a prime and $q \neq p$, then for any $\mathfrak{q} \in \mathfrak{P}$ such that divides q, $M_{\mathfrak{q}} = \mathbb{Z}_{\mathfrak{q}}$. Now suppose

$$p = \prod_{\mathfrak{p}|p} \tilde{\mathfrak{p}}^{e(\mathfrak{p}|p)}$$

is the factorization of p in K. Then $e(\mathfrak{p}|p) \leq p-1$, so $p \nmid e(\mathfrak{p}|p)$. It follows ([14], p. 302) that $\delta(\mathfrak{p}|p) = e(\mathfrak{p}|p) - 1$. Hence, we obtain

$$p-2 = \sum_{\mathfrak{P}|p} f(\mathfrak{P}|p)(e(\mathfrak{P}|p)-1)$$

$$= \sum_{\mathfrak{P}|p} f(\mathfrak{P}|p)e(\mathfrak{P}|p) - \sum_{\mathfrak{P}|p} f(\mathfrak{P}|p)$$

$$= (p-1) - \sum_{\mathfrak{P}|p} f(\mathfrak{P}|p),$$

since

$$p-1 = \sum_{\mathfrak{P}|p} f(\mathfrak{P}|p)e(\mathfrak{P}|p).$$

So $f(\mathfrak{P}|p) = 1$, and $p = \tilde{\mathfrak{P}}^{p-1}$. We then see that $d_p = p$ and $d_q = 1$. Therefore, $d_{K|\Omega}(M)$ is square-free. Moreover, $M = (1-\zeta)^{-h}$, where ζ is a primitive p^{th} root of unity and $h = (p-3)/2$. This follows since $\mathfrak{P} = (1-\zeta)$, and $\delta(\mathfrak{P}|p) = p-2$, so $[\delta/2] = (p-3)/2$.

IV. The Discriminant of Almost-Fundamental Modules

Throughout this chapter we shall assume that F is either the rational field Q or a p-adic field. If $a, b \in F$, then $(a, b)_p$ will denote the Hilbert symbol of a and b with respect to p; and if A is an F-matrix, $C_p(A)$ will denote the Hasse-symbol of A. The Hilbert symbol, the Hasse symbol, and their properties are presented in [8]; we assume these properties. We shall also make use of the following technical lemma.

Lemma. If $A = \mathrm{diag}[a_1, a_2, \ldots, a_n]$, then

$$C_p(A) = \prod_{i \le j} (a_i, a_j)_p \ .$$

Proof: We will need this only for odd primes p, and so we assume that p is odd. We have

$$C_p(A) = (-1, A_n)_p \prod_{i<n} (A_i, -A_{i+1})_p \ ,$$

where A_i is the determinant of the principal i-rowed minor. When A is diagonal,

$$A_i = \prod_{k \le i} a_k \ ,$$

so

$$\begin{aligned} (A_i, -A_{i+1})_p &= \Big(\prod_{k \le i} a_k, \ - \prod_{k \le i} a_k \cdot a_{i+1} \Big)_p \\ &= \Big(\prod_{k \le i} a_k, \ - \prod_{k \le i} a_k \Big)_p \Big(\prod_{k \le i} a_k, \ a_{i+1} \Big)_p \\ &= \Big(\prod_{k \le i} a_k, \ a_{i+1} \Big)_p = \prod_{k \le i} (a_k, a_{i+1})_p \ . \end{aligned}$$

Also,

$$(-1, -\prod_{k\le n} a_k)_p = (-1, \prod_{k\le n} a_k)_p = \prod_{k\le n} (a_k, -1)_p = \prod_{k\le n} (a_k, a_k)_p \ .$$

Hence,

$$C_p(A) = \prod_{1<i\le n} \prod_{k<i} (a_k, a_i)_p \prod_{j\le n} (a_j, a_j)_p$$

$$= \prod_{i\le n} \prod_{k\le i} (a_k, a_i)_p = \prod_{j\le i} (a_j, a_i)_p \ .$$

In order to prove the main theorem of this chapter, we apply a method used by G. Pall to prove a similar result in case $F = Q$. Although Pall's proof is as yet unpublished, the result appears in [4], and the technique was sketched for me by D. Estes.

4.1 Theorem. Suppose that M is a $\mathbb{Z}_F$-module with an n-element $\mathbb{Z}_F$-basis σ, and suppose that $D(\sigma)$ is integral. Then M is almost-fundamental if and only if the following conditions are satisfied:

(a) If p is an odd prime, $p^3 \nmid d_{K|F}(M)$; and if $p^2 \mid d_{K|F}(M)$, then $C_p(D(\sigma)) = -1$.

(b) If $2^t \parallel d_{K|F}(M)$, then $0 \le t \le 1$.

Proof: (I) First define an "inner product" $(\cdot\ ,\ \cdot)$ on K in the following way. For each $x, y \in K$, let

$$(x, y) = S_{K|F}(xy) \ .$$

We see that M is not almost-fundamental if and only if the following condition holds: there is an $m \in K$, $m \notin M$ such that $(m, M) \subseteq \mathbb{Z}_F$ and $(m, m) \in \mathbb{Z}_F$. For then the module $M^* = M + m\mathbb{Z}_F$ properly contains M and the trace of the product of any two elements of M^* is integral. Since $M^* \supseteq M$, the module M^* has an n-element $\mathbb{Z}_F$-basis and so must have an integral discriminant matrix. We wish to ex-

press this condition in terms of the matrix $D(\underline{\sigma})$ and therefore we will express the inner product (x, y) as follows. For each $x \in K$ write

$$x = x_1\sigma_1 + \ldots + x_n\sigma_n \; ; \; x_i \in F .$$

Then let $\hat{x}$ denote the column vector

$$\hat{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Since $D(\underline{\sigma}) = (S_{K|F}(\sigma_i\sigma_j))$, an easy calculation shows that

$$(x, y) = \hat{x}' D(\underline{\sigma})\hat{y} . \tag{4.2}$$

Now suppose that there is an element $m \in K$, $m \notin M$ and such that $(m, M) \subseteq \mathbb{Z}_F$ and $(m, m) \in \mathbb{Z}_F$. Write

$$m = \frac{x_1\sigma_1 + \ldots + x_n\sigma_n}{d} ,$$

where the x_i and d belong to $\mathbb{Z}_F$, and d does not divide every x_i. Let p be a prime divisor of d and let $d = pd'$. Now set $m' = d'm$. Then $m' \notin M$ but $x = pm' \in M$. The following conditions are then fulfilled:

(i) $\hat{x} \not\equiv 0 \pmod{p}$ (that is, not every entry is divisible by p)

(ii) $(x, M) \equiv 0 \pmod{p}$

(iii) $(x, x) \equiv 0 \pmod{p^2}$.

Conversely, suppose we can find an $x \in M$ which satisfies (i), (ii), and (iii) for some prime p. Then let $m = x/p$. Clearly, $m \notin M$ but $(m, M) \subseteq \mathbb{Z}_F$ and $(m, m) \in \mathbb{Z}_F$. Therefore, we see that M is almost fundamental if and only if conditions (i), (ii), and (iii) cannot be

satisfied for any prime p and any $x \in M$. By (4.2) conditions (i), (ii), and (iii) can be written as

$$\hat{x} \not\equiv 0 \pmod{p}$$

$$\hat{x}'D(\underline{\sigma}) \equiv 0 \pmod{p} \tag{4.3}$$

$$\hat{x}'D(\underline{\sigma})\hat{x} \equiv 0 \pmod{p^2}.$$

Hence, we have shown that M is almost-fundamental if and only if (4.3) does not hold for any prime p and any integral vector $\hat{x}$. Note that (4.3) has a rational integral solution $\hat{x}$ if and only if it has a p-adic integral solution $\hat{y}$, for we can write $\hat{y} = \hat{x} + p^{\alpha}\hat{z}$ where $\hat{x}$ is a rational integral vector and $\hat{z}$ is a p-adic integral vector. If we choose $\alpha \geq 2$, then $\hat{x}$ must satisfy (4.3). Therefore, M is almost-fundamental if and only if there is no prime p such that (4.3) has a p-adic integral solution $\hat{x}$. It is this last formulation that we will use throughout the remainder of the proof.

(II) Suppose M is almost-fundamental. We now show that (a) and (b) are necessary. First, suppose p is an odd prime. Then there is an integral (p-adic integral) unimodular matrix U such that $U'D(\underline{\sigma})U$ is diagonal ([8], p. 84). Now (4.3) has an integral solution if and only if it does with $D(\underline{\sigma})$ replaced by $U'D(\underline{\sigma})U$. And the Hasse symbol remains invariant under this transformation. Hence, we can assume $D(\underline{\sigma})$ is diagonal.

If p^3 divides $\det D(\underline{\sigma})$, then $D(\underline{\sigma})$ is one of the following:

$$\begin{bmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & p^3 a_n \end{bmatrix}, \quad \begin{bmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & pa_{n-1} \\ & & & & p^2 a_n \end{bmatrix} \quad \text{or}$$

$$\begin{bmatrix} a_1 & & & & 0 \\ & a_2 & & & \\ & & \ddots & & \\ & & & pa_{n-1} & \\ 0 & & & & pa_n \end{bmatrix} ,$$

where, in the last case, a_{n-2}, a_{n-1}, and a_n are not divisible by p. In the first two cases it is evident that

$$\hat{x} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

will satisfy 4.3. In the third case, there will be an x satisfying 4.3 if the congruence

$$a_{n-2}x^2 + a_{n-1}y^2 + a_n z^2 \equiv 0 \pmod{p}$$

has a non-trivial solution. But this congruence can be rewritten as

$$(-a_n a_{n-2})x^2 + (-a_n a_{n-1})y^2 \equiv z^2 \pmod{p} ,$$

and since $(-a_n, a_{n-2}, -a_n a_{n-1})_p = 1$, the congruence does have a non-trivial solution. Therefore, $p^3 \nmid \det D(\underline{\sigma})$.

Assume that $p^2 \parallel \det D(\underline{\sigma})$. Then $D(\underline{\sigma})$ is one of the following:

$$\begin{bmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & p^2 a_n \end{bmatrix} , \text{ or } \begin{bmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & pa_{n-1} \quad pa_n \end{bmatrix} ,$$

where no a_i is divisible by p. By the argument used above, $D(\underline{\sigma})$ must be of the second form. In the second case, M is not almost-fundamental if the congruence

$$a_{n-1}x^2 + a_n y^2 \equiv 0 \pmod{p}$$

has a non-trivial solution. There are non-trivial solutions if and only if $\left(\frac{-a_{n-1}a_n}{p}\right) = 1$, where $\left(\frac{-}{p}\right)$ is the Legendre symbol. We can express this condition in terms of $C_p(D(\underline{\sigma}))$ as follows. Since $D(\underline{\sigma})$ is diagonal, we apply the lemma at the beginning of the chapter to obtain

$$C_p(D(\underline{\sigma})) = \prod_{i\le n-2} (a_i, pa_{n-1})_p \cdot \prod_{i\le n-2} (a_i, pa_n)_p (pa_{n-1}, pa_{n-1})_p (pa_n, pa_n)_p (pa_{n-1}, pa_n)_p$$

$$= (pa_{n-1}, pa_n)_p = \left(\frac{-a_{n-1}a_n}{p}\right) .$$

So it is necessary that $C_p(D(\underline{\sigma})) = -1$.

Now suppose that $p = 2$. We cannot assume that $D(\underline{\sigma})$ is diagonal, but we may take ([8], pp. 84, 85)

$$D(\underline{\sigma}) = \begin{bmatrix} A & & & 0 \\ & B_1 & & \\ & & B_2 & \\ 0 & & & \ddots \end{bmatrix}$$

where A, B_1, B_2, ... are integral block matrices. The matrix A is diagonal, and the B_i are 2×2 blocks of one of the following types:

$$\begin{bmatrix} 2^{t_i} & 2^{t_i-1} \\ 2^{t_i-1} & 2^{t_i} \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 0 & 2^{t_i-1} \\ 2^{t_i-1} & 0 \end{bmatrix} .$$

If 2^2 divides $\det A$, then A can be written in one of the following forms:

$$\begin{bmatrix} a_1 & & & & 0 \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_{k-1} & \\ 0 & & & & 2^2 a_k \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} a_1 & & & & 0 \\ & a_2 & & & \\ & & \ddots & & \\ & & & 2a_{k-1} & \\ 0 & & & & 2a_k \end{bmatrix} ,$$

where in the second case a_{n-1} and a_n are not divisible by 2. In the first case it is clear that

$$\hat{x} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

(where the 1 occurs in the k^{th} position) is a solution of 4.3. In the second case, we can find a solution $\hat{x}$ if the congruence

$$a_{k-1}x^2 + a_k y^2 \equiv 0 \pmod 2$$

has a non-trivial solution. Since a_{k-1} and a_k are both odd, it does have a non-trivial solution. We therefore reach a contradiction unless <u>at most</u> one entry in A is divisible by 2.

If, for any block B_i, $t_i > 1$, then

$$2^{t_i}x^2 + 2^{t_i}xy + 2^{t_i}y^2 \equiv 0 \pmod 4$$

or

$$2^{t_i}xy \equiv 0 \pmod 4$$

has a non-trivial solution, and hence 4.3 does also. Therefore, each $t_i = 1$, and $|\det B_i| = 1$. Hence, if $2^t \parallel \det D(\underline{\sigma})$, then $0 \le t \le 1$.

(III) Now assume that (a) and (b) are satisfied. We must show that there is no prime p and no integral $\hat{x}$ which satisfies 4.3. Again, if p = 2 we may take

$$D(\underline{\sigma}) = \begin{bmatrix} A & & & \\ & B_1 & & \\ & & B_2 & \\ & & & \ddots \end{bmatrix}.$$

Then each of the blocks B_i must be such that $t_i = 1$; hence, if $t > 0$, one of the entries in A must be divisible by 2, and A must have the form

$$\begin{bmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & 2^t a_n \end{bmatrix}$$

with each $a_i \equiv 1 \pmod 2$, and $0 \leq t \leq 1$. For A, B_1, B_2, ... satisfying these conditions, it is not possible to find an $\hat{x}$ which will satisfy 4.3 .

If p is odd, and $p \nmid \det D(\underline{\sigma})$, then $D(\underline{\sigma})$ has the form

$$\begin{bmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{bmatrix}$$

where each $a_i \not\equiv 0 \pmod p$. Clearly, there is no $\hat{x}$ which satisfies 4.3 . If $p \parallel \det D(\underline{\sigma})$ a similar argument suffices to show that there is no $\hat{x}$ satisfying 4.3 . Finally, suppose $p^2 \parallel \det D(\underline{\sigma})$. Then $C_p(D(\underline{\sigma})) = -1$, and $D(\underline{\sigma})$ can be put into one of the following forms:

$$\begin{bmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & pa_n \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & p^2 a_n \end{bmatrix},$$

where each $a_i \not\equiv 0 \pmod p$. By computing the Hasse-symbol for each of these forms, we see that $D(\underline{\sigma})$ must be of the first type. Now there is an $\hat{x}$ satisfying 4.3 only if

$$a_{n-1}x^2 + a_n y^2 \equiv 0 \pmod p$$

has a non-trivial solution; but in view of the condition $C_p(D(\underline{\sigma})) = -1$, this is not possible.

We have proved 4.1 .

V. Normal Almost-Fundamental Fields

Suppose that $K|F$ is an extension of F which satisfies the conditions imposed in Chapter III.

5.1 Definition. The field $K|F$ is said to be almost-fundamental if $\mathbb{Z}_K$ is almost-fundamental.

5.2 Theorem. If $K_{\mathfrak{P}}|F_{\mathfrak{p}}$ is an extension of the complete field F, then K is almost-fundamental if and only if the differential exponent satisfies

$$\delta(\mathfrak{P}|\mathfrak{p}) \leq 1 .$$

Proof: Immediate from 3.6.

In the remainder of this chapter we assume that $F = Q$, the rational field, and we study normal almost-fundamental extensions. The results of section 3a are restated in the next theorem.

5.3 Theorem. If $K|Q$ is quadratic, then K is almost-fundamental if and only if $K = Q(\sqrt{D})$, where $D \equiv 1 \pmod 4$.

We now prove the following theorem.

5.4 Theorem. If $K|Q$ is normal and almost-fundamental, then $K|Q$ is quadratic or non-cyclic of degree four.

Proof: For any almost-fundamental extension $K|Q$ we have, in view of 3.19,

$$\sum_{\mathfrak{P}|p} f(\mathfrak{P}|p)\mu(\mathfrak{P}|p) = \sum_{\mathfrak{P}|p} f(\mathfrak{P}|p)\delta(\mathfrak{P}|p)$$

for each prime divisor p of the discriminant $d_{K|Q}$. Now in view of the definition (p. 33) of $\mu(\mathfrak{P}|p)$, it is clear that

$$\mu(\mathfrak{P}\,|p) \leq \delta(\mathfrak{P}\,|p) .$$

Hence,

$$0 = \sum_{\mathfrak{P}\,|p} f(\mathfrak{P}\,|p)[\delta(\mathfrak{P}\,|p) - \mu(\mathfrak{P}\,|p)]$$

implies that

$$\mu(\mathfrak{P}\,|p) = \delta(\mathfrak{P}\,|p) .$$

Now ([14], p. 302)

$$\delta(\mathfrak{P}\,|p) \geq e(\mathfrak{P}\,|p) - 1 \geq 0$$

with equality on the left if and only if p does not divide $e(\mathfrak{P}\,|p)$. We see that if $\delta(\mathfrak{P}\,|p)$ is even it must be zero, and then $e(\mathfrak{P}\,|p) = 1$. If $\delta(\mathfrak{P}\,|p)$ is odd then $\delta(\mathfrak{P}\,|p) = 1$, and $e(\mathfrak{P}\,|p) = 2$. In this case $p \neq 2$.

Now assume that $K|Q$ is a normal extension. Then for every pair $\mathfrak{P}$, $\mathfrak{Q}$ of divisions of p, $e(\mathfrak{P}\,|p) = e(\mathfrak{Q}|p)$ and $f(\mathfrak{P}\,|p) = f(\mathfrak{Q}|p)$. It follows that $e(\mathfrak{P}\,|p) = 2$ for every $\mathfrak{P}\,|p$. But if e and f are the common values of $e(\mathfrak{P}\,|p)$ and $f(\mathfrak{P}\,|p)$, respectively, and g is the number of divisors of p, then

$$n = [K:Q] = efg ,$$

and so 2 must divide $[K:Q]$. Now by 3.19 and 4.1 we must have

$$\sum_{\mathfrak{P}\,|p} f(\mathfrak{P}\,|p)\delta(\mathfrak{P}\,|p) = \sum_{\mathfrak{P}\,|p} f(\mathfrak{P}\,|p) \leq 2 .$$

So the possible factorizations of p in $\mathbb{Z}_K$ are the following:

(a') $p = \tilde{\mathfrak{P}}^2$, $\qquad f(\mathfrak{P}\,|p) = 2$ or 1

(b') $p = \tilde{\mathfrak{P}}_1^2\,\tilde{\mathfrak{P}}_2^2$ $\qquad f(\mathfrak{P}_i|p) = 1 .$

Since n is even, we see that $n = 2$ or $n = 4$. The case $n = 2$ has been dealt with in 5.3 ; we therefore suppose that $n = 4$.

Let L be a quadratic subfield of K. Then L must be almost-fundamental, for $\mathfrak{d}_{K|Q} = \mathfrak{d}_{K|L} \cdot \mathfrak{d}_{L|Q}$, and by taking norms we obtain

$$d_{K|Q} = N_{L|Q}(d_{K|L}) \cdot d_{L|Q}^2 . \tag{5.5}$$

Since 2 does not divide $d_{K|Q}$, and $d_{K|Q}$ has at most square factors, it follows that 2 does not divide $d_{L|Q}$ and so $d_{L|Q}$ is square-free.

We now show that K must contain more than one quadratic subfield. Suppose it is not true, and let L be the unique quadratic subfield. For each $\mathfrak{P}|p$ we have shown that $e(\mathfrak{P}|p) = 2$, and so since $e(\mathfrak{P}|p)$ is the degree of K over the inertial field of $\tilde{\mathfrak{P}}$ ([14], p. 292), and L is the unique quadratic subfield, it follows that L must be the inertial field of $\tilde{\mathfrak{P}}$. In view of (a') and (b'), we see that p factors in $\mathfrak{Z}_L$ in one of the following ways:

$$p = \tilde{\mathfrak{P}}$$

or

$$p = \tilde{\mathfrak{P}}_1 \, \tilde{\mathfrak{P}}_2 .$$

In either case, p is unramified in L. But in view of 5.5, we see that it is possible to choose p so that p divides both $d_{K|Q}$ and $d_{L|Q}$, in which case p must ramify in L. Hence, we are led to a contradiction. Therefore, K contains two distinct quadratic subfields: $L_i = Q(\sqrt{D_i})$, $D_i \equiv 1 \pmod 4$, (for $i = 1, 2$).

If $(D_1, D_2) = 1$, we can prove the following:

5.6 Theorem. If D_1 and D_2 are relatively prime, then the field $K = Q(\sqrt{D_1}, \sqrt{D_2})$ is almost-fundamental if and only if the following conditions are satisfied:

(a) D_1 and $D_2 \equiv 1 \pmod 4$

(b) If p and q are primes such that p divides D_2 and q divides D_1, then

$$\left(\frac{-D_1}{p}\right) = \left(\frac{-D_2}{q}\right) = -1 .$$

Proof: We have already shown that condition (a) is necessary. In order to show that (b) is necessary, we now determine an integral basis for $K|Q$.

Since $D_1 \equiv 1 \pmod 4$, then $\left(1, \frac{1+\sqrt{D_1}}{2}\right)$ is an integral basis for $L_1|Q$. Further, we shall show that it is also an integral basis for $K|L_2$. Let

$$\mathcal{O} = \mathbb{Z}_{L_2} \oplus \frac{1+\sqrt{D_1}}{2}\,\mathbb{Z}_{L_2} .$$

The discriminant matrix of $\mathcal{O}$ over L_2 is

$$\begin{bmatrix} 2 & 1 \\ 1 & \frac{1+D_1}{2} \end{bmatrix} ;$$

it is integral, and $d_{K|L_2}(\mathcal{O}) = (D_1)$ is square-free in Q. Further, (D_1) has no square factors in $\mathbb{Z}_{L_2}$, for we can write

$$D_1\mathbb{Z}_Q = (p_1)(p_2)\cdots(p_r) ,$$

where the p_i are distinct primes; hence

$$D_1\mathbb{Z}_{L_2} = (p_1\mathbb{Z}_{L_2})\cdots(p_r\mathbb{Z}_{L_2}) .$$

Now p_i does not divide $d_{L_2|Q} = D_2$ and so is unramified in $\mathbb{Z}_{L_2}$; therefore the prime ideal factors of $D_1\mathbb{Z}_{L_2}$ are distinct.

Now $\mathcal{O} \subseteq \mathbb{Z}_K$, and we have just shown that $d_{K|L_2}(\mathcal{O})$ is

square-free, so $\mathcal{O}$ cannot be properly contained in a $\mathbb{Z}_{L_2}$-module with integral discriminant.[4] Therefore, $\mathcal{O} = \mathbb{Z}_K$. From this, it follows that

$$1, \quad \frac{1+\sqrt{D_1}}{2}, \quad \frac{1+\sqrt{D_2}}{2}, \quad \frac{1+\sqrt{D_1}}{2} \cdot \frac{1+\sqrt{D_2}}{2}$$

is an integral basis for $K|Q$.

Using the results of the preceding paragraph, we are able to compute the discriminant of the field:

$$d_{K|Q} = N_{L_1|Q}(d_{K|L_1}) d_{L_1|Q}^2$$

$$= N_{L_1|Q}(D_2) D_1^2 = (D_1 D_2)^2 .$$

We now apply 4.1 to the matrix

$$D(\underline{\omega}) = \begin{bmatrix} 4 & 2 & 2 & 1 \\ 2 & 1+D_1 & 1 & \frac{1+D_1}{2} \\ 2 & 1 & 1+D_2 & \frac{1+D_2}{2} \\ 1 & \frac{1+D_1}{2} & \frac{1+D_2}{2} & \frac{1+D_1}{2}\,\frac{1+D_2}{2} \end{bmatrix},$$

where $\underline{\omega}$ is the integral basis for $K|Q$ which was determined above. Let δ_i be the principal i-rowed minor determinant; then

$$\delta_1 = 4, \quad \delta_2 = 4D_1, \quad \delta_3 = 4D_1 D_2, \quad \delta_4 = (D_1 D_2)^2,$$

and [8]

---

[4] Although $\mathbb{Z}_K$ may not have a 2-element $\mathbb{Z}_{L_2}$-basis, one can define its discriminant as in [3], page 11. Then the conclusion above follows from [3], proposition 4, page 12.

$$C_p(D(\underline{\omega})) = (-1, -\delta_4)_p \prod_{i=1}^{3}{}' (\delta_i, -\delta_{i+1})$$

$$= (1, -D_1)_p (D_1, -D_1D_2)_p (D_1D_2, -1)_p .$$

If $q \mid D_1$, then

$$C_q(D(\underline{\omega})) = \left(\frac{-D_2}{q}\right) ;$$

and if $p \mid D_2$, then

$$C_p(D(\underline{\omega})) = \left(\frac{-D_1}{p}\right) .$$

In view of 4.1, we must have

$$\left(\frac{-D_1}{p}\right) = \left(\frac{-D_2}{q}\right) = -1 .$$

The sufficiency of conditions (a) and (b) follows from 4.1 and the fact that we can use the argument above to show that $d_{K \mid Q} = (D_1D_2)^2$.

5.5 Example. $Q(\sqrt{5}, \sqrt{13})$ is almost-fundamental, but $Q(\sqrt{13}, \sqrt{17})$ is not.

References

[1] E. Artin, Theory of Algebraic Numbers, Göttingen notes, Göttingen, 1959.

[2] E. Bender, Symmetric Representations of an Integral Domain Over a Subdomain, Ph. D. thesis, California Institute of Technology, Pasadena, 1966.

[3] J. W. S. Cassels and A. Fröhlich, Algebraic Number Theory, Thompson Book Co., Inc., 1967.

[4] D. Estes and G. Pall, Modules and Rings in the Cayley Algebra, to appear in the Journal of Number Theory.

[5] D. K. Faddeev, On the Characteristic Equations of Rational Symmetric Matrices, Dokl. Akad. Nauk USSR (N. S.) 58 (1947), 753-754.

[6] H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin, 1963.

[7] T. Husain, Introduction to Topological Groups, W. B. Saunders Co., 1966.

[8] B. W. Jones, The Arithmetic Theory of Quadratic Forms, Carus Monographs, Math. Assoc. Amer., 1950.

[9] W. J. LeVeque, Topics in Number Theory, Vol. II, Addison Wesley, 1956.

[10] O. T. O'Meara, Introduction to Quadratic Forms, Academic Press, Inc., 1963.

[11] O. Taussky, On the Similarity Transformation between an Integral Matrix with Irreducible Characteristic Polynomial and Its Transpose, Math. Annalen 166 (1966), 60-63.

[12] O. Taussky, Ideal Matrices I, Archiv der Mathematiks 13 (1962), 275-282.

[13] O. Taussky, The Discriminant Matrices of an Algebraic Number Field, J. London Math. Soc. 43 (1968), 152-154.

[14] O. Zariski and P. Samuel, Commutative Algebra, Vol. I, University Series in Higher Mathematics, Van Nostrand Co., Inc., 1958.