Extensions

Let A be a noetherian domain which is integrally closed in its field of fractions K. Let L/K be a finite field extension with $n = [L : K]$ and let B be the integral closure of A in L. We want to know under what conditions is B a finitely generated A-module. The following proposition gives one such condition:

Proposition 0.1. *If L/K is separable, then B is a finitely generated A-module.*

Proof. We first define a symmetric non-denerate K-bilinear form $\langle \cdot, \cdot \rangle \colon L \times L \to K$ as follows: given $y, y' \in L$, we set

$$\langle y, y' \rangle := \mathrm{Tr}_{L/K}(yy').$$

Indeed, it is clearly symmetric and bilinear since the usual multiplication map on L is symmetric and K-bilinear and since the trace map is K-linear. Recall that $\mathrm{Tr}_{L/K} = 0$ if and only if L/K is nonseparable. Equivalently, $\mathrm{Tr}_{L/K}$ is onto if and only if L/K is separable. Since L/K is separable, there exists a $\widetilde{y} \in L$ such that $\mathrm{Tr}_{L/K}(\widetilde{y}) \neq 0$. In particular, if $y \neq 0$ is in L, then $\langle y, y^{-1}\widetilde{y} \rangle \neq 0$, hence $\langle \cdot, \cdot \rangle$ is non-degenerate as well. We claim that the trace map restricted to B lands in A. To see this, we first choose a finite extension L'/L such that L'/K is Galois. Then for each $b \in B$ we have

$$\mathrm{Tr}_{L/K}(b) = \sum_{\sigma \colon L \hookrightarrow L'} \sigma(b) \tag{1}$$

where the sum in L' is taken over all K-embeddings $\sigma \colon L \hookrightarrow L'$. Each $\sigma(b)$ is integral over A since b is integral over A, and thus the sum (1) is also integral over A. Since $\mathrm{Tr}_{L/K}(b) \in K$ and is integral over A, it follows that $\mathrm{Tr}_{L/K}(b) \in A$. Now for each $y \in L$, we obtain a K-linear map $\ell_y \colon L \to K$ where $\ell_y(y') = \langle y, y' \rangle$ for all $y' \in L$. Given an A-submodule M of L, we set

$$M^\vee = \{y \in L \mid \ell_y(M) \subseteq A\} = \{y \in L \mid \langle y, u \rangle \in A \text{ for all } u \in M\}.$$

Suppose that $e_1, \dots, e_n$ is a K-basis of L, and by rescaling the e_i if necessary, we may also assume that each e_i is in B. For each i, we let $e_i^\vee$ be the unique element in L such that

$$\langle e_i^\vee, e_j \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases}$$

Indeed, $e_i^\vee$ is unique precisely because $\langle \cdot, \cdot \rangle$ is non-degenerate. If we set $F = \sum_i Ae_i$ to be the free A-module spanned by the e_i, then clearly we have $F^\vee = \sum_i Ae_i^\vee$. Furthermore we have inclusions:

$$F \subseteq B \subseteq B^\vee \subseteq F^\vee.$$

In particular, B is contained in a finitely generated A-module, and since A is noetherian, it follows that B is a finitely generated A-module. □

Remark 1. The condition stated in the proposition above is not the only condition that implies B is a finitely generated A-module. One can show that if A is a finitely generated $\Bbbk$-algebra where $\Bbbk$ is a field, then B is a finitely generated A-module. Similarly one can show that if A is a complete discrete valuation ring, then B is a finitely generated A-module.

For now on, we now assume that B is finitely generated as an A-module. We also assume that $\dim A = 1$, hence A is a Dedekind domain. This implies $\dim B = 1$ since B is integral over A, and thus B is a Dedekind domain too. In this case, if we are given a nonzero prime $\mathfrak{p}$ of A, then we have a decomposition

$$\mathfrak{p}B = \prod_{\mathfrak{q} \mid \mathfrak{p}} \mathfrak{q}^{e_\mathfrak{p}}$$

where the $e_\mathfrak{q} \in \mathbb{Z}_{\geq 0}$ are uniquely determined. Since there are only

Proposition 0.2.

Discriminant

Let K be a field and let R be a finite dimensional K-algebra which is also finite as a K-vector space. Then there is a canonical symmetric K-bilinear map $\langle \cdot, \cdot \rangle \colon R \times R \to K$ given by

$$\langle r, r' \rangle = \mathrm{Tr}_{R/K}(rr')$$

for all $r, r' \in R$. We call $\langle \cdot, \cdot \rangle$ the **trace product** of R/K. The the reason why the trace product of R/K is useful is because it can help us determine the structure of R as a K-algebra. Indeed, in general R will be isomorphic as a K-algebra to a direct product of fields

$$R \simeq L_1 \times L_2 \times \cdots \times L_m,$$

where L_i/K is a finite extension. Then in this case, the trace product will decompose as

$$\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_1 + \langle \cdot, \cdot \rangle_2 + \cdots + \langle \cdot, \cdot \rangle_m,$$

where $\langle \cdot, \cdot \rangle_i$ corresponds to the trace product of the field extension L_i/K. More specifically, if $r, r' \in R$, then we set

$$\langle r, r' \rangle_i = \begin{cases} \langle r, r' \rangle & \text{if } r, r' \in L_i \\ 0 & \text{else} \end{cases}$$

Moreover, if L_i/K is not separble, then $\langle \cdot, \cdot \rangle_i = 0$, and if L_i/K is separable, then $\langle \cdot, \cdot \rangle_i|_{L_i \times L_i}$ is non-degenerate and agrees with the trace product of L_i/K.

Now suppose K is the field of fractions of a dedekind domain A, and that A is integrally closed in K. Let L/K be a finite extension of fields and let B be the integral closure of A in L. Then the trace product of L/K has the following nice property:

1. When we restrict to entries in B, we land in A (you prove this by using the description of the trace function as a sum of embeddings formula). Thus the trace product of L/K restricts to the trace product of B/A.

2. Suppose $\mathfrak{q}$ is a prime ideal of B which lies over a prime ideal $\mathfrak{p}$ of A. Also set $\mathbb{k}_{\mathfrak{q}} = B/\mathfrak{q}$ and $\mathbb{k} = A/\mathfrak{p}$, so we have an extension $\mathbb{k}_{\mathfrak{q}}/\mathbb{k}_{\mathfrak{p}}$ of finite fields. When we restrict to entries in $\mathfrak{q}$, we land in $\mathfrak{q}$. Furthermore, if we restrict one entry in $\mathfrak{p}$ and the other entry in $\mathfrak{q}$, then we land in $\mathfrak{p}$. Thus the trace product of trace product of B/A and this is a lift of the trace product of $\mathbb{k}_{\mathfrak{q}}/\mathbb{k}_{\mathfrak{p}}$.

In particular, let $\boldsymbol{e} = e_1, \ldots, e_n$ be a K-basis of L such that each e_i is in B, and let $\boldsymbol{e}^\vee = e_1^\vee, \ldots, e_n^\vee$ be the dual basis of $\boldsymbol{e}$ with respect to $\langle \cdot, \cdot \rangle$, that is

$$\langle e_i, e_j^\vee \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases}$$