M3P8 LECTURE NOTES 12: INTEGERS IN NUMBER FIELDS

1. Integer Rings

Let K be a finite extension of $\mathbb{Q}$. Such an extension is called a *number field.* The integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is called the *ring of integers* of K.

A fundamental result of number theory is that $\mathcal{O}_K$ is a Dedekind domain. The goal of this section is to prove this fact. Indeed, we will prove something more general, but in order to do that we need to introduce some new concepts.

2. Trace and Norm

Let L/K be a finite extension, and let α be an element of L. Then we can regard L as a finite-dimensional K-vector space. Multiplication by α is then a K-linear map from L to L. If we choose a K-basis for L, such a map is given by a d by d matrix M_α, with entries in K where d is the degree of L over K. The matrix of course depends on the basis chosen, but its trace and determinant are elements of K that depend only on α. We denote the trace of M_α by $\operatorname{Tr}_{L/K} \alpha$ and call it the *trace* of α with respect to L/K. Similarly, the determinant of M_α is denoted $N_{L/K}\alpha$ and called the *norm* of α.

Lemma 2.1. *The map $\alpha \mapsto \operatorname{Tr}_{L/K} \alpha$ is K-linear: if $\alpha, \beta \in L$, and $c \in K$, then*

$$\operatorname{Tr}_{L/K} c\alpha + \beta = c \operatorname{Tr}_{L/K} \alpha + \operatorname{Tr}_{L/K} \beta.$$

The map $N_{L/K}$ is multiplicative:

$$N_{L/K}(\alpha\beta) = (N_{L/K}\alpha)(N_{L/K}\beta)$$

Proof. Distributivity of multiplication over addition shows that, with respect to a fixed basis of L over K, $M_{c\alpha+\beta} = cM_\alpha + M_\beta$. Similarly $M_{\alpha\beta} = M_\alpha M_\beta$, by associativity of multiplication. The claims thus follow from the linearity of trace and multiplicativity of determinant. □

Proposition 2.2. *Let L/K be a finite extension, and α an element of L. Let $Q(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be the minimal polynomial of α over K. Then:*

- $\operatorname{Tr}_{L/K} \alpha = -da_{n-1}$, *and*
- $N_{L/K}\alpha = ((-1)^n a_0)^d$,

where d is the degree of L over $K(\alpha)$.

Proof. We first prove this when $d = 1$. Then $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ is a basis for L over K. With respect to this basis M_α has the matrix:

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

From which both claims can be easily deduced. In general choose a basis $\beta_1, \dots, \beta_d$ for L over $K(\alpha)$. Then

$$\beta_1, \beta_1\alpha, \dots, \beta_1\alpha^{n-1}, \beta_2, \beta_2\alpha, \dots, \beta_d, \beta_d\alpha, \dots, \beta_d\alpha^{n-1}$$

is a basis for L/K. With respect to this basis M_α is block diagonal, consisting of d blocks along the diagonal, each of which is the n by n matrix above. The claim follows. □

Remark 2.3. The map $\operatorname{Tr}_{L/K} \to K$ is sometimes the zero map. However, this does not happen if K has characteristic zero or if the degree d of L/K is relatively prime to the characteristic of K, since the above proposition shows that $\operatorname{Tr}_{L/K} 1 = d$.

3. The main result

We can now state our main result.

Theorem 3.1. *Let R be a PID with field of fractions K, and let L/K be a finite extension such that $\operatorname{Tr}_{L/K}$ is not the zero map. Let S be the integral closure of R in L. THen S is a Dedekind domain.*

To prove this, we must show three things about S: that S is Noetherian, that S is integrally closed, and that every nonzero prime ideal of S is maximal. We first show:

Lemma 3.2. *The field of fractions of S is L.*

Proof. In fact, we'll show that every element of L can be expressed as $\frac{s}{r}$ for $s \in S$ and $r \in R$. Let $\alpha \in L$, and let $P(X)$ be the minimal polynomial of α over K. Let d be the degree of $P(X)$. For each $r \in R$, let $P_r(X) = r^d P(\frac{X}{r})$; we can seen we can find an r such that $P_r(X)$ has coefficients in R. But $P_r(X)$ is the minimal polynomial of $r\alpha$, so it follows that for such r, $r\alpha$ is integral over R and thus lies in X. □

Corollary 3.3. *The ring S is integrally closed.*

Proof. We have shown that the integral closure S of R in L is integrally closed in L; since L is the field of fractions of S, we have that S is integrally closed. □

Next we show that S is Noetherian. In fact, we will show that S is a finitely generated R-module; since R is Noetherian it will then follow that S is Noetherian as an R-module, and hence also as an S-module.

To do this, we consider the map $L \times L \to K$ defined by $\langle x, y\rangle = \mathrm{Tr}_{L/K}\, xy$. This pairing is symmetric (that is, $\langle x, y\rangle = \langle y, x\rangle$) and K-bilinear: if $x_1, x_2, y \in L$, and $\lambda \in K$, then $\langle x_1 + \lambda x_2, y\rangle = \langle x_1, y\rangle + \lambda\langle x_2, y\rangle$. It is also *perfect*: since we have assumed that $\mathrm{Tr}_{L/K}$ is not the zero map, there exists $z \in L$ such that $\mathrm{Tr}_{L/K}\, z$ is nonzero in K; then given any nonzero $x \in L$, we have $\langle x, zx^{-1}\rangle \neq 0$.

Now choose a basis $\beta_1, \dots, \beta_d$ for L over K. We have seen that for each i there exists $r_i \in R$ such that $r_i\beta_i \in S$, so (replacing β_i by $r_i\beta_i$) we may assume that the β_i all lie in S. Since the pairing $\langle , \rangle$ is perfect, there also exist $\gamma_1, \dots, \gamma_d \in S$ such that $\langle \beta_i, \gamma_j\rangle = 1$ if $i = j$ and 0 otherwise. Then the elements $\gamma_1, \dots, \gamma_d$ also form a basis for L over K, called the *dual basis* to $\beta_1, \dots, \beta_d$.

Let M be the R-module spanned by the β_i, and let M^* denote the subset of S consisting of all s such that $\langle s, m\rangle$ lies in R for all $m \in M$.

First note that M^* is an R-module; it is closed under addition and multiplication by R because the pairing $\langle , \rangle$ is R-bilinear. Moreover, the elements $\gamma_1, \dots, \gamma_d$ all lie in M^*, and form a basis for M^* over R. To see this, first note that any $m \in M$ can be written as $\sum_i r_i\beta_i$ with $r_i \in R$, so that $\langle \gamma_j, m\rangle = r_j$, which certainly lies in R. Thus $\gamma_1, \dots, \gamma_d$ lie in M^*. They are certainly R-linearly independent, as they are K-linearly independent. So it suffices to show that they span M^*. Given $m \in M^*$, let $r_i = \langle m, \beta_i\rangle$ for all i, and let $m' = \sum_i r_i\gamma_i$. Then $\langle m - m', \beta_i\rangle = 0$ for all i, so $m - m' = 0$.

Finally, note that $M \subseteq S \subseteq M^*$, since for any $m \in M$, sm lies in S and thus its trace lies in R. Thus S is an R-submodule of the finitely generated R-module M^*, and (since R is Noetherian), S is therefore finitely generated as an R-module.

Now it remains to prove that every nonzero prime ideal of S is maximal. Let I be a nonzero prime ideal of S, and let α be an element of I. Let $Q(X)$ be the minimal polynomial of α over K; then $Q(X)$ has coefficients in R. We then have:

$$0 = Q(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n$$

where $a_0, \dots, a_{n-1}$ are the coefficients of $Q(X)$ (and thus lie in R). Rewriting, we get:

$$-a_0 = \alpha(a_1 + a_2\alpha + \cdots + a_{n-1}\alpha^{n-2} + \alpha^{n-1})$$

In particular $-a_0$ lies in the ideal generated by α, and hence in I. Moreover, since $Q(X)$ is irreducible, a_0 is a nonzero element of R.

Consider the intersection $J = I \cap R$. Then J is a prime ideal of R, and J is nonzero since $a_0 \in J$. Thus J is a *maximal* ideal of R. The ring S/I is an integral domain containing the field R/J. Moreover, since S is a finitely generated R-module, S/I is a finitely generated R/J-module; that is, S/I is a finite dimensional R/J-vector space. We now show:

Lemma 3.4. *Let F be a field and let T be an integral domain containing F that is finite dimensional as an F-vector space. Then T is a field.*

Proof. Let α be a nonzero element of T, and let $P(X)$ be the minimal polynomial of α over F. Then we can write $0 = a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}+\alpha^n$, with $a_i \in F$ the coefficients of P. Since T is an integral domain, $P(X)$ is irreducible, so $a_0 \neq 0$. Then

$$\alpha^{-1} = a_0^{-1}(a_1 + a_2\alpha + \cdots + a_{n-1}\alpha^{n-2} + \alpha^{n-1})$$

gives a multiplicative inverse for α in T. □

The lemma shows that S/I is a field, so I is maximal.

We have thus shown that S is Noetherian, integrally closed, and that every nonzero prime ideal in S is maximal, so S is indeed a Dedekind domain.

In particular, for any finite extension $K/\mathbb{Q}$, the integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is a Dedekind domain (and thus has unique factorization of ideals).

Another class of examples comes by taking K a field, letting L be a finite extension of $K(t)$ such that $\mathrm{Tr}_{L/K(t)}$ is nonzero, and letting R be the integral closure of $K[t]$ in L. The field L is called a *function field*, and the ring R is the "ring of regular functions on a smooth affine algebraic curve". Such rings R are also Dedekind domains, and they are of considerable interest in algebraic geometry. They of course also have the unique factorization property for ideals, and just like in ring of integers one can consider the ideal class group. In this context, the ideal class group is also known as the *Picard group* - it has a geometric interpretation in terms of line bundles on algebraic curves. Unlike in the number field setting, the Picard group is often not a finite group.