ZAHLENTHEORIE SS 2019 - NOTE 4

We want to study number fields and their rings of integers in a systematic way. We begin with a useful observation

Rmk: Any number field can be written as $K = \mathbb{Q}(\alpha)$, where α is integral over $\mathbb{Z}$.

proof: we know that $K = \mathbb{Q}(\bar{\alpha})$ for a certain $\bar{\alpha} \in K$.
Since $K/\mathbb{Q}$ is finite, $\bar{\alpha}$ is algebraic over $\mathbb{Q}$, hence

$$\bar{\alpha}^n + \frac{a_{n-1}}{b_{n-1}}\bar{\alpha}^{n-1} + \dots + \frac{a_1}{b_1}\bar{\alpha} + \frac{a_0}{b_0} = 0$$

for $a_i, b_j \in \mathbb{Z}$. We multiply by b^n, where $b = b_0 \cdot b_1 \cdot \dots \cdot b_{n-1}$ and we get

$$(b\bar{\alpha})^n + a_{n-1}\frac{b}{b_{n-1}}(b\bar{\alpha})^{n-1} + \dots + a_1 \cdot \frac{b^{n-1}}{b_1}(b\bar{\alpha}) + a_0\frac{b}{b_0} = 0$$

So that $\alpha := b\cdot\bar{\alpha}$ is integral over $\mathbb{Z}$.
To conclude we observe that $\mathbb{Q}(\bar{\alpha}) = \mathbb{Q}(b\bar{\alpha})$. □

Hence, from now on when we write $K = \mathbb{Q}(\alpha)$, we will always take α integral over $\mathbb{Z}$.

---

§. TRACE and NORM

Two useful tools to study number fields and their rings of integers are the trace and the norm. We can define them generally as follows:

def: TRACE and NORM

Let K/F be a finite field extension.

For any $\alpha \in K$, consider the K-linear map

$$(\cdot\alpha): K \longrightarrow K$$
$$x \longmapsto \alpha x$$

We define the trace and the norm of α as

$$Tr_{K/F}(\alpha) = \text{trace of } (\cdot\alpha)$$
$$N_{K/F}(\alpha) = \text{determinant of } (\cdot\alpha)$$

This defines two maps

$$Tr_{K/F}: K \to F$$
$$N_{K/F}: K \to F$$

(0) If $\alpha \in F$, then $Tr_{K/F}(\alpha) = [K:F]\alpha$ $N_{K/F}(\alpha) = \alpha^{[K:F]}$.

Example: (1) Consider the extension $F(\alpha)/F$ where α has minimal polynomial

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$$

What are the trace and the norm of α?

We consider the basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ of $F(\alpha)$ and then we write the matrix representing the multiplication $(\cdot\alpha): F(\alpha) \to F(\alpha)$ w.r.t.

this basis. We get

$$\alpha \cdot 1 = \alpha$$
$$\alpha \cdot \alpha = \alpha^2$$
$$\alpha \cdot \alpha^2 = \alpha^3$$
$$\vdots$$
$$\alpha \cdot \alpha^{n-1} = \alpha^n = -a_{n-1}\alpha^{n-1} - \dots - a_1\alpha - a_0$$

hence the matrix is

$$(\cdot\alpha) \rightsquigarrow \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ & & & 0 & -a_{n-2} \\ 0 & 0 & & 1 & -a_{n-1} \end{pmatrix}$$

We compute the trace and norm and we get

$$Tr(\alpha) = -a_{n-1}$$
$$N(\alpha) = (-1)^n a_0$$

Rmk: In general we can look at the characteristic polynomial of the map $(\cdot\alpha)$: this is given by

$$\det \begin{pmatrix} t & & & a_0 \\ -1 & t & & \vdots \\ & -1 & \ddots & \\ & & t & a_{n-2} \\ & & -1 & t+a_{n-1} \end{pmatrix} = m_\alpha(t)$$

Hence, all the coefficients of the minimal

polynomials give us informations on α.
However, trace and norm are the most interesting because of the following

Lemma: The trace is additive and the norm is multiplicative, meaning that if L/K is a finite extension, then

$$Tr_{K/F}(\alpha+\beta) = Tr_{K/F}(\alpha) + Tr_{K/F}(\beta)$$
$$N_{K/F}(\alpha\beta) = N_{K/F}(\alpha) N_{K/F}(\beta)$$

proof: Let's look at the multiplication maps $\cdot(\alpha+\beta)$ and $\cdot(\alpha\beta)$. It is clear that

$$\cdot(\alpha+\beta) = (\cdot\alpha) + (\cdot\beta), \quad \cdot\alpha\beta = (\cdot\alpha)\circ(\cdot\beta)$$

(composition)

Then we conclude because the trace is additive on matrices and the determinant is multiplicative. □

Thm: Let K/F be a finite field extension and let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \overline{F}$ be all possible embeddings s.t. $\sigma_i|_F = id_F$. Then

$$Tr_{K/F}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha) \quad \forall \alpha \in K$$
$$N_{K/F}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$$

proof: Suppose first that $K = F(\alpha)$. Then we know

that the minimal polynomial of α over F is

$$m_\alpha(X) = (X-\sigma_1(\alpha))(X-\sigma_2(\alpha))\cdots(X-\sigma_n(\alpha))$$
$$= X^n - (\sigma_1(\alpha)+\cdots+\sigma_n(\alpha))X^{n-1} + \cdots + (-1)^n$$

Hence by our remark of before $\sigma_1(\alpha)\cdots\sigma_n(\alpha)$ we get

$$\sigma_1(\alpha)+\cdots+\sigma_n(\alpha) = \mathrm{Tr}_{K/F}(\alpha)$$
$$\sigma_1(\alpha)\cdots\sigma_n(\alpha) = N_{K/F}(\alpha)$$

Now consider $K \geq F(\alpha) \geq F$: if

$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is the basis of $F(\alpha)$ over F

and $\beta_1, \ldots, \beta_m$ is a basis of K over $F(\alpha)$, then

$\beta_1, \alpha\beta_1, \ldots, \alpha^{n-1}\beta_1$ is a basis of

$\beta_2, \alpha\beta_2, \ldots, \alpha^{n-1}\beta_2$ K/F

$\vdots \quad \vdots \quad \vdots$

$\beta_m, \alpha\beta_m, \ldots, \alpha^{n-1}\beta_m$

We compute the matrix of the multiplication by $\cdot\alpha$ w.r.t. this basis: we see that

$$\alpha \cdot \alpha^i\beta_j = \alpha^{i+1}\beta_j \quad \text{if} \quad i < n-1$$
$$\alpha \cdot \alpha^n\beta_j = -a_{n-1}\alpha^{n-1}\beta_j - \cdots - a_1\alpha\beta_j - a_0\beta_j$$

Hence, the matrix is a block matrix:

$$\begin{pmatrix} \begin{bmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{n-1} \end{bmatrix} & 0 & \cdots & 0 \\ 0 & \begin{bmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{n-1} \end{bmatrix} & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \begin{bmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{n-1} \end{bmatrix} \end{pmatrix}$$

$$\begin{pmatrix} & & & \\ & \ddots & 0 & \\ & & 1 & -a_{n-1} \end{pmatrix}$$

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

So we see that

$$Tr_{K/F}(\alpha) = m \cdot Tr_{F(\alpha)/F}(\alpha)$$

$$N_{K/F}(\alpha) = \left(N_{F(\alpha)/F}(\alpha)\right)^m$$

Now, consider the embeddings

$$\sigma_i : F(\alpha) \hookrightarrow \overline{F} \quad \text{s.t.} \quad \sigma_i|_F = id$$

Each one of these can be extended to m other embeddings

$$\tau_{ij} : K \hookrightarrow \overline{F} \quad \text{s.t.} \quad \tau_{ij}|_{F(\alpha)} = \sigma_i$$

Since these are n.m embeddings which restrict to the identity on F, these are all the embeddings. Hence

$$Tr_{K/F}(\alpha) = \sum_i \sum_j \tau_{ij}(\alpha) = \sum_i \sum_j \sigma_i(\alpha) =$$

$$= m \cdot \left(\sum_i \sigma_i(\alpha)\right) = m \cdot Tr_{F(\alpha)/F}(\alpha)$$

$$N_{K/F}(\alpha) = \prod_i \prod_j \tau_{ij}(\alpha) = \prod_i \prod_j \sigma_i(\alpha)$$

$$= \left(\prod_i \sigma_i(\alpha)\right)^m = N_{F(\alpha)/F}(\alpha)^m$$

Which proves what we want. □

The phenomenon that we have seen in this proof generalizes

Thm: Let $L \supseteq K \supseteq F$ be field extensions. Then

$$Tr_{L/F} = Tr_{K/F} \circ Tr_{L/K}$$
$$N_{L/F} = N_{K/F} \circ N_{L/K}$$

proof: suppose first that L/F is normal. Then

as before, let $\sigma_1, \dots, \sigma_n$ be all the embeddings $\sigma_i : K \hookrightarrow \overline{F}$ s.t. $\sigma_i|_F = id_F$

If $m = [L:K]$ then each one of those can be extended to $\tau_{ij} : L \hookrightarrow \overline{F}$ s.t. $\tau_{ij}|_F = \sigma_i$.

So, these are $n \cdot m$ embeddings of L in $\overline{F}$ which leave F fixed pointwise. Since $[L:F] = nm$, these are all the embeddings. One of the σ_i must be id_F: we can set $\sigma_1 = id_F$. Then for $\alpha \in L$ we have

$$Tr_{L/F}(\alpha) = \sum_{i=1}^{n} \sum_{j=1}^{m} \tau_{ij}(\alpha) =$$

$$(Tr_{K/F} \circ Tr_{L/K})(\alpha) = Tr_{F/L}\left(\sum_{j=1}^{m} \tau_{1j}(\alpha)\right) =$$

$$= \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \tau_{1j}(\alpha)\right) = \sum_{i=1}^{n} \tau_{i1}\left(\sum_{j=1}^{m} \tau_{1j}(\alpha)\right)$$

$n \quad m$

$$= \sum_{i=1}^{m} \sum_{j=1}^{m} (\tau_{i1} \circ \tau_{1j})(\alpha) \qquad (*)$$

Observe that the composition makes sense because L/F is normal. To conclude, observe that if $x \in K$, then

$$(\tau_{i1} \circ \tau_{1j})(x) = \tau_{i1}(\sigma_1(x)) = \tau_{i1}(x) = \sigma_i(x)$$

So $\tau_{i1} \circ \tau_{1j}$ restricts to σ_i on K, and moreover if $j_1 \neq j_2$ we also have $\tau_{i1} \circ \tau_{1j_1} \neq \tau_{i1} \circ \tau_{1j_2}$ hence, the sets

$$\{\tau_{ij} \mid j = 1, \dots, m\}, \{\tau_{i1} \circ \tau_{1j} \mid j = 1, \dots, m\}$$

coincide, and we see that

$$(*) = \sum_{i=1}^{m} \sum_{j=1}^{m} \tau_{ij}(\alpha) = \mathrm{Tr}_{L/F}(\alpha).$$

If L/F is not normal, then, let $M \supseteq L \supseteq K \supseteq F$ its normal closure. From what we have already proven we have

$$\mathrm{Tr}_{M/F}(\alpha) = \mathrm{Tr}_{L/F}(\mathrm{Tr}_{M/L}(\alpha))$$
$$\mathrm{Tr}_{M/F}(\alpha) = \mathrm{Tr}_{K/F}(\mathrm{Tr}_{M/K}(\alpha))$$

Moreover, we have that

- $\mathrm{Tr}_{M/L}(\alpha) = [M:L]\alpha$, since $\alpha \in L$
- $\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha))$
  $= [M:L]\,\mathrm{Tr}_{L/K}(\alpha)$

Hence, we get

$$[M:L]\,Tr_{L/F}(\alpha) = [M:L]\,Tr_{K/F}\left(Tr_{L/K}(\alpha)\right)$$

which is what we want. For the norm the same holds. □

In particular, if we look at the trace, we see that it can also be seen as a bilinear form

$$\begin{aligned} Tr_{K/F} : K \times K &\longrightarrow F \\ (\alpha, \beta) &\longmapsto Tr_{K/F}(\alpha\beta) \end{aligned}$$

of F-vector spaces. Equivalently, this is a map

$$\begin{aligned} Tr'_{K/F} : K &\longrightarrow \mathrm{Hom}_F(K, F) \\ \alpha &\longmapsto Tr_{K/F}(\alpha\,\cdot) : K \longrightarrow F \\ &\qquad\qquad \beta \longmapsto Tr_{K/F}(\alpha\beta) \end{aligned}$$

This is a nice bilinear form:

Thm: Suppose K/F is separable. Then the bilinear form $Tr_{K/F}$ is nondegenerate. This means, equivalently, that

(a) there is no $x \neq 0$ s.t. $Tr_{K/F}(xy) = 0$ $\forall y \in K$

(b) the map $Tr_{K/F} : K \longrightarrow \mathrm{Hom}(K, F)$ is an isomorphism of F-vector spaces.

proof: first we prove that (a) holds. Indeed if there is $x \neq 0$, then for each $\alpha \in K$ we have

$\mathrm{Tr}_{K/F}(\alpha) = \mathrm{Tr}_{K/F}(\chi(\chi^{-1}\alpha)) = 0$.

Hence, it is enough to prove that $\mathrm{Tr}_{K/F}$ is not identically zero, however, $\mathrm{Tr}_{K/F}(1) = [K:F] \neq 0$

The fact that (a), (b) are equivalents standard:

indeed

(a) $\Rightarrow$ (b): (a) means precisely that the map $K \to \mathrm{Hom}_F(K, F)$ is injective, and since the two spaces have the same finite dimension, it is an isomorphism.

(b) $\Rightarrow$ (a) if $K \to \mathrm{Hom}_F(K, F)$ is an isomorphism then it is injective, and this means precisely (a). □

• INTEGRAL ELEMENTS

Now we put rings of integers back into the picture.

Rmk: R = integral domain

$K \supseteq F \supseteq R$ fields.

Let $\sigma: K \hookrightarrow \overline{F}$ be an embedding s.t. $\sigma|_F = \mathrm{id}_F$.

If $\alpha \in K$ is integral over R, then $\sigma(\alpha)$ is also integral over R.

proof: Let $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$ be with coefficients in R. Then

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

□

because $\sigma(a_i)=a_i$. Then $\sigma(a)$ is integral over K.

Prop: R = integrally closed domain (e.g. $R=\mathbb{Z}$)
F = Frac R (e.g. $\mathbb{Q}$)
$K \supseteq F$ finite extension (e.g. K = number field)
$\overline{R}$ = integral closure of R in K (e.g. $\mathcal{O}_K$)

Then $\mathrm{Tr}_{L/K}(\alpha) \in R$, $N_{L/K}(\alpha) \in R$ for all $\alpha \in \overline{R}$.

proof: Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \overline{F}$ be the embeddings of K s.t. $\sigma_i|_K = \mathrm{id}_F$. If $\alpha \in R$, then

$$\mathrm{Tr}_{K/F}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$$
$$N_{K/F}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$$

are both integral over R, because all the $\sigma_i(\alpha)$ are. Moreover we know that they are both in F, and since R is integrally closed, it follows that both are in R. □

For example, we can generalize a fact that we have seen many times in examples: the norm characterizes invertible elements.

Prop: R = integrally closed domain ($R=\mathbb{Z}$)
F = Frac R ($F=\mathbb{Q}$)
$K \supseteq F$ finite extension (K = number field)

$\overline{R}$ = integral closure of R in K ($\overline{R} = \mathcal{O}_K$)

Then

$$\alpha \in \overline{R}^* \iff N_{K/F}(\alpha) \in R^*$$

proof: ($\Rightarrow$) Suppose $\alpha\beta = 1$ for $\alpha, \beta \in \overline{R}^*$. Then $N_{K/F}(\alpha) N_{K/F}(\beta) = 1$ and we know that these are both in R.

($\Leftarrow$) Suppose there is $u \in R$ s.t.

$$N_{K/F}(\alpha) \cdot u = 1$$

Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \overline{F}$ be all embeddings s.t. $\sigma_i|_K = id_F$. We also set $\sigma_1 = id_K$. Then we get

$$\alpha \cdot \sigma_2(\alpha) \cdots \sigma_n(\alpha)\, u = 1$$

and it is enough to prove that $\sigma_2(\alpha) \cdots \sigma_n(\alpha) \in \overline{R}$. We know that this is integral over R, so it is enough to show that $\sigma_2(\alpha) \cdots \sigma_n(\alpha) \in K$. To do this:

$$\sigma_2(\alpha) \cdots \sigma_n(\alpha) = N_{K/F}(\alpha) \cdot \alpha^{-1}.$$

($N_{K/F}(\alpha) \in F$, $\alpha^{-1} \in K$) □

A very important consequence of the trace, instead, is that number rings are finitely generated over $\mathbb{Z}$. More precisely we have

Thm (FINITENESS of INTEGRAL CLOSURE)

R = noetherian integrally closed domain (e.g. $R=\mathbb{Z}$)
$F = \mathrm{Frac}\, R$ (e.g. $F=\mathbb{R}$)
$K \supseteq F$ finite extension (e.g. K = number field)
$\overline{R}$ = integral closure of R in K (e.g. $\overline{R}=\mathcal{O}_K$)

Then $\overline{R}$ is finite over R.

There is the new word "noetherian" in the statement: we define it here

def: NOETHERIAN RINGS and MODULES

A module M over a ring R is called noetherian if one of the following equivalent conditions are satisfied:

(i) every submodule of M is finitely generated

(ii) for every ascending sequence

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots \subseteq M_n \subseteq M_{n+1} \subseteq \dots$$

of submodules, we have that

$$M_n = M_{n+1} \text{ for } n \gg 0.$$

A ring R is called noetherian if it is noetherian as a module over itself. Equivalently, this means:

(i') every ideal of R is finitely generated.

(ii') for every ascending sequence

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq I_{n+1} \subseteq \dots$$

of ideals, we have that
$I_n = I_{n+1}$ for $n \gg 0$.

Example: (1) $\mathbb{Z}$ is noetherian, and in general every PID is noetherian.
(2) A field K is noetherian.
(3) A non-noetherian ring is the ring of polynomials in infinitely many variables: $R = K[x_1, x_2, \ldots]$ where K is a field.

Properties: Some important properties of noetherianity are
(1) Let M be a noetherian R-module. Then submodules $M' \subseteq M$, and quotients $M'' = M/M'$ of M are noetherian.
(2) If M, N are noetherian R-modules, then $M \oplus N$ is noetherian.
(3) Let R be a noetherian ring and M an R-module. M is noetherian $\iff$ M is finitely generated as an R-module as an R-module.

Now we can prove the theorem:

proof of finitedness of integral closure: first write $K = F(\alpha)$, with α integral over R. Then we have a basis of K over F given by

$\alpha_0 = 1, \alpha_1 = \alpha, \dots, \alpha_{n-1} = \alpha^{n-1}$ ...

which are all integral elements over R.

Now, since the trace $Tr_{K/F}$ is nondegenerate, the map

$$Tr_{K/F} : K \longrightarrow Hom_F(K, F)$$

is an isomorphism, so that there is a basis $\beta_0, \beta_1, \dots, \beta_{n-1}$ of K over F s.t.

$$Tr_{K/F}(\alpha_i \beta_j) = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

This is called a DUAL BASIS of the original basis α_i.

Now, let $x \in \overline{R}$. Then we can write

$$x = x_0 \beta_0 + \dots + x_{n-1} \beta_{n-1} \quad \text{for certain } x_i \in F.$$

If we multiply by α_i we get

$$\alpha_i x = x_0(\alpha_i \beta_0) + \dots + x_i(\alpha_i \beta_i) + \dots + x_{n-1}(\alpha_i \beta_{n-1})$$

hence

$$Tr_{K/F}(\alpha_i x) = \sum_{j=0}^{n-1} Tr_{K/F}(x_j(\alpha_i \beta_j)) =$$

$$= \sum_{j=0}^{n-1} x_j \cdot Tr_{K/F}(\alpha_i \beta_j) =$$

$$= \sum_{j=0}^{n-1} x_j \delta_{ij} = x_i$$

And since $\alpha_i x \in \overline{R}$, we get

$$x_i = Tr_{K/F}(\alpha_i x) \in R \quad \forall i$$

Since this holds for every $x \in \overline{R}$ we see that

$$\overline{R} \subseteq R\beta_0 + \dots + R\beta_{n-1}$$ this is the R-module

↖ generated by $\beta_0, \dots, \beta_{n-1}$

Since R is noetherian and the module $R\beta_0 + \dots + R\beta_{n-1}$ is finitely generated, we get that $R\beta_0 + \dots + R\beta_{n-1}$ is noetherian, and the sub module $\overline{R}$ is also finitely generated. □

° THE RING of INTEGERS of a NUMBER FIELD

When we deal with rings of integers, we can be much more precise about the structure of $\mathcal{O}_K$ as a $\mathbb{Z}$-module. The point is that finitely generated modules over $\mathbb{Z}$ (i.e. finitely generated abelian groups) have a very simple description:

Thm: CLASSIFICATION of f.g. MODULES over PID

Let R be a PID and let

Let M be a finitely generated R-module.

Then

$$M \cong R^{\oplus r} \oplus R/d_1R \oplus \dots \oplus R/d_sR$$

where $r \geq 0$ and the $d_i \in R$, $d_i \neq 0$ are s.t.

$$d_1 \mid d_2 \mid \dots \mid d_s$$

Moreover, the r and the d_i are uniquely determined. The r is called the RANK of M.

proof: In the Exercise sheet

Rmk:

(1) If M is a f.g. R-module, then its torsion part is defined as

$$M_{tor} = \{ m \in M \mid \exists a \in R, a \neq 0 \text{ s.t. } am = 0 \}$$

This is a submodule of M, and in the above description we see that

$$M_{tor} \cong R/d_1 \oplus \dots \oplus R/d_k .$$

(2) If M is torsion free, then the theorem tells us that M is FREE. This is exactly like saying that M has a basis: a set of linearly independent generators over R. Indeed, let

$$\varphi : R^{\oplus r} \longrightarrow M \text{ be an isomorphism}$$

The module

$$R^{\oplus r} = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_r \end{bmatrix} \mid a_i \in R \right\}$$

has a standard basis given by

$$e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i\text{-th position}$$

and then φ is an isomorphism $\Leftrightarrow$ $\varphi(e_1), \dots, \varphi(e_n)$ is a basis for M.

(3) If M is torsion-free, then every submodule

$N \subseteq M$ is also torsion-free, and moreover

$$\operatorname{rank}(N) \leq \operatorname{rank}(M)$$

(this is a bit like the dimension for vector spaces)

proof: It is clear that N is torsion-free.

We need to prove $\operatorname{rank}(N) \leq \operatorname{rank}(M)$.

Thanks to the theorem, we can suppose $M \cong R^{\oplus r}$.

Now, suppose that there is a submodule $N \subseteq R^{\oplus r}$ of rank $> r$. If we take a basis of N, then we get linearly independent elements $v_1, \dots, v_s \in R^{\oplus r}$ with $s > r$. Let now $F = \operatorname{Frac}(R)$. Then $R^{\oplus r} \subseteq F^{\oplus r}$, and the $v_1, \dots, v_s$ must be linearly dependent over F (since we are dealing with usual linear dependence over a field). This means that

$$\frac{a_1}{b_1} v_1 + \dots + \frac{a_s}{b_s} v_s = 0 \quad \text{in } F^{\oplus r}$$

for some $a_i, b_i \in R$. However, we can multiply this by $b = b_1 \cdots b_s$ and we get

$$\left(\frac{b}{b_1} \cdot a_1\right) v_1 + \dots + \left(\frac{b}{b_s} \cdot a_s\right) \cdot v_s = 0$$

and since the $\frac{b}{b_i} a_i \in R$, we see that the $v_1, \dots, v_s$ are linearly dependent over R.

With this we can give the structure of number rings as $\mathbb{Z}$-modules

Thm: Let K be a number field. Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$.

proof: this follows from the same strategy of the previous proof. First, let us write $K = \mathbb{Q}(\alpha)$ for α integral over $\mathbb{Z}$. Then

$$\alpha_0 = 1,\ \alpha_1 = \alpha, \dots, \alpha_{n-1} = \alpha^{n-1}$$

is a basis of K over $\mathbb{Q}$, where $n = [K:\mathbb{Q}]$.

We also have a dual basis $\beta_0, \beta_1, \dots, \beta_{n-1}$ s.t.

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \beta_j) = \delta_{ij}$$

and we have proven in the finiteness theorem that

$$\mathcal{O}_K \subseteq \mathbb{Z}\beta_0 + \mathbb{Z}\beta_1 + \dots + \mathbb{Z}\beta_{n-1}$$

Moreover, since the α_i are integral over $\mathbb{Z}$, we also have

$$\mathbb{Z}\alpha_0 + \dots + \mathbb{Z}\alpha_{n-1} \subseteq \mathcal{O}_K \subseteq \mathbb{Z}\beta_0 + \dots + \mathbb{Z}\beta_{n-1}$$

Now we observe that since the α_i and the β_j are linearly independent over $\mathbb{Q}$, they are also linearly independent over $\mathbb{Z}$, hence

$\mathbb{Z}\alpha_0 + \dots + \mathbb{Z}\alpha_{n-1}$ and $\mathbb{Z}\beta_0 + \dots + \mathbb{Z}\beta_{n-1}$ are free $\mathbb{Z}$-modules of rank n

Then it follows that $\mathcal{O}_K$ is also free, and

$$\underbrace{\mathrm{rk}(\mathbb{Z}\alpha_0 + \dots + \mathbb{Z}\alpha_{n-1})}_{= n} \leq \mathrm{rk}(\mathcal{O}_K) \leq \underbrace{\mathrm{rk}(\mathbb{Z}\beta_0 + \dots + \mathbb{Z}\beta_{n-1})}_{= n}$$

$\square$

Rmk: Since $\mathcal{O}_K$ is free over $\mathbb{Z}$, it has a basis.
Any such basis is called an INTEGRAL BASIS.

Example: (1) $K = \mathbb{Q}(\sqrt{d})$, d sqfr

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \ (4) \\ \mathbb{Z}[\sqrt{d}], & d \equiv 2, 3 \ (4) \end{cases}$$

Then, an integral basis of $\mathcal{O}_K$ is given by

$1, \frac{1+\sqrt{d}}{2}$ $\quad d \equiv 1 \ (4)$.

$1, \sqrt{d}$ $\quad d \equiv 2, 3 \ (4)$.