Thm 3.68: $R$ a principal ideal domain, $L$ a finite separable extension of $K := Q(R)$, $S := R^{\mathrm{int},L}$. Then every finitely generated $S$-submodule $V \neq 0$ of $L$ is free as an $R$-module and $\dim_R V = \dim_K L$.
This applies in particular to $S$ and any ideal of $S$.

Proof:

$R$ a PID $\Rightarrow$ $R$ integrally closed by Exercise 3.2 ($R$ factorial)
Can thus apply Thm 3.47 $\leadsto$ $S$ is a f.g. $R$-module.
$\leadsto$ $V$ a f.g. $R$-module
$\leadsto$ $V$ a free $R$-module by Thm 3.66 since $V \subseteq L$ and $L$ torsion-free $R$-module.
Remains to prove claim about dimension.

Let $V = R\cdot\{\beta_1, \dots, \beta_n\}$. Since $V \subseteq L$ and $Q(S) = L$, there is $s \in S\setminus\{0\}$ s.t. $s\beta_i \in S \;\forall i$ $\Rightarrow$ $sV \subseteq S$

In the proof of Thm 3.47 we have seen that there is a $K$-basis $\{\alpha_1, \dots, \alpha_n\}$ of $L$ with $\alpha_i \in S$ such that

dual basis

$$R\cdot\{\alpha_1, \dots, \alpha_n\} \subseteq S \subseteq R\cdot\{\alpha_1', \dots, \alpha_n'\}$$

$$\Rightarrow \quad sV \subseteq S \subseteq R\cdot\{\alpha_1', \dots, \alpha_n'\}.$$

$sV$ is a finitely generated $R$-module, it is torsion-free (since a submodule of $L$) $\Rightarrow$ $sV$ is a free $R$-module.
Since $sV \cong V$, same for $V$.
By above $\quad \dim_R V = \dim_R sV \leq n = \dim_K L$

Recall, $V = R\cdot\{\beta_1, .., \beta_n\}$.

Let $j$ such that $\beta_j \neq 0$. Since $V$ is an $S$-module, $\alpha_i \in S$ and $\beta_j \in V$

$\Rightarrow$ $\beta_j\alpha_i \in V$ $\forall i$ $\Rightarrow$

Since the $\{\alpha_1, .., \alpha_n\}$ linearly independent over $R$

and $\beta_j \neq 0$, so is $\{\beta_j\alpha_1, .., \beta_j\alpha_n\}$

$\Rightarrow$ $n \leq \dim_R V$

$\Rightarrow$ $\dim_R V = n = \dim_K L$ $\square$

<u>Cor</u> 3.69: $L$ a number field. Then $\mathcal{O}_L$, and any ideal in $\mathcal{O}_L$, is a free $\mathbb{Z}$-module of dimension $= \dim_{\mathbb{Q}} L$. $\square$

<u>Def</u> 3.70: A $\mathbb{Z}$-basis of $\mathcal{O}_L$ is called an <u>integral basis</u>.

<u>Goal</u>: Find such a basis!

Need some tools to work with free modules and bases.

Let $V$ be a f.g. free $R$-module ($R$ a PID). Fix a basis $\{v_1, .., v_m\}$ of $V$.

If $U \subseteq V$ is a submodule $\rightsquigarrow$ $U$ free. Choose a basis $\{u_1, .., u_n\}$.

Can represent $U$ by the matrix $A \in \mathrm{Mat}_{m\times n}(R)$ of the embedding $U \hookrightarrow V$ in the bases.

Depends on choice of basis of $U$ of course.

But: can transform $A$ to a canonical form! $\rightsquigarrow$ allows us, e.g., for $U, U' \subseteq V$ to test for equality $U = U'$, inclusion $U \subseteq U'$, compute $U + U'$, etc.

# 4. Hermite and Smith normal form

Let $R$ be a PID. Let us fix:

- $P$, a <u>complete set of non-associates</u> of $R$, i.e. a set of representatives of $r \sim r' \Leftrightarrow r = ur'$ for some unit $u \in R$.
- $P(r)$ for each $r \in R$, a <u>complete set of residues modulo $r \in R$</u>, i.e. a set of representatives of $R/(r)$

<u>Ex</u> 4.1: In $R = \mathbb{Z}$ we always choose $P = \mathbb{Z}_{\geq 0}$, $P(r) = \{0, 1, \dots, |r|-1\}$.
If $R = K$ is a field, choose $P = \{0, 1\}$, $P(r) = \{0\}$ $\forall r$

<u>Def</u> 4.2: $A = (a_{ij}) \in Mat_{m \times n}(R)$ is in <u>Hermite normal form</u> (HNF) if $A = 0$, or if $A \neq 0$ and there is $r$, $1 \leq r \leq m$, such that

1. $row_i(A) \neq 0$ $\forall 1 \leq i \leq r$, $row_i(A) = 0$ $\forall i \geq r+1$
2. there is a sequence $1 \leq n_1 < n_2 < \dots < n_r \leq m$ such that for each $i$, $1 \leq i \leq r$,

   a) : $a_{ij} = 0$ $\forall j < n_i$

   b) : $a_{in_i} \in P \setminus \{0\}$

   c) $a_{jn_i} \in P(a_{in_i})$

So, $A$ looks like

$$
\begin{array}{cc}
 & \begin{array}{ccccccccc} \phantom{0 \cdots 0} & n_1 & \phantom{* \cdots *} & n_2 & \phantom{* \cdots *} & n_3 & \phantom{* \cdots *} & n_r & \phantom{* \cdots *} \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow & \end{array} \\
\begin{array}{c} \\ \\ \\ \\ r \rightarrow \\ \\ \\ \\ \end{array} &
\begin{pmatrix}
0 \cdots 0 & a_{1n_1} & * \cdots * & a_{1n_2} & * \cdots * & a_{1n_3} & * \cdots * & a_{1n_r} & * \cdots * \\
0 \cdots 0 & 0 & 0 \cdots 0 & a_{2n_2} & * \cdots * & a_{2n_3} & * \cdots * & a_{2n_r} & * \cdots * \\
0 \cdots 0 & 0 & 0 \cdots 0 & 0 & 0 \cdots 0 & a_{3n_3} & * \cdots * & a_{3n_r} & * \cdots * \\
\vdots \quad \vdots & \vdots & & \vdots & & \vdots & \vdots & \vdots & \\
0 \quad 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & a_{rn_r} & * \cdots * \\
0 \quad 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 \cdots 0 \\
\vdots \quad \vdots & \vdots & & \vdots & & \vdots & & \vdots & \vdots \quad \vdots \\
0 \quad 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 \quad 0
\end{pmatrix}
\end{array}
$$

<u>Ex:</u>[4.3] $\begin{pmatrix} 2 & 1 & 0 & 21 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & 56 \end{pmatrix} \in Mat_3(\mathbb{Z})$ is in HNF

<u>Remark:</u>[4.4] If $R=K$ is a field the HNF is the reduced row echelon form.

<u>Thm:</u>[4.5] For any $A \in Mat_{m\times n}(R)$ there is $U \in GL_m(R)$ such that $U\cdot A$ is in HNF.
The HNF of $A$ is uniquely determined.

We illustrate how to get the HNF in an example. It will be clear that this works generally $\Rightarrow$ proves existence of HNF. We skip the proof of uniqueness (but it's elementary).

<u>Ex:</u>[4.6]

is non-zero; otherwise exchange rows first

$$A = \begin{array}{c} \\ p= \\ b= \\ \\ \end{array}\begin{pmatrix} 4 & 2 & 9 & 5 \\ 6 & 3 & 4 & 3 \\ 8 & 4 & 1 & -1 \end{pmatrix}$$

want to make this zero

Let $g = \gcd(b,p)$ and write $g = xp + yb$

Consider

$$U = \begin{pmatrix} x & y \\ \frac{b}{g} & -\frac{p}{g} \end{pmatrix} \rightsquigarrow \det U = -\left(x\frac{p}{g} + y\frac{b}{g}\right) = -1$$
$$\rightsquigarrow U \in GL(R)$$

Apply this to $A$, i.e. replace

$$row_1(A) \rightsquigarrow x\, row_1(A) + y\, row_2(A)$$
$$row_2(A) \rightsquigarrow \frac{b}{g} row_1(A) - \frac{p}{g} row_2(A)$$

This will kill $b$!

In the example: $\gcd(4,6) = 2 = -1\cdot 4 + 1\cdot 6 \rightsquigarrow U = \begin{pmatrix} -1 & 1 \\ 3 & -2 \end{pmatrix}$

$$\longrightarrow \begin{pmatrix} 2 & 1 & -5 & -2 \\ 0 & 0 & 19 & 9 \\ 8 & 4 & 1 & -1 \end{pmatrix}$$

$\gcd(2,8) = 2 = 1\cdot 2 + 0\cdot 8$

$\rightsquigarrow U = \begin{pmatrix} 1 & 0 \\ 4 & -1 \end{pmatrix}$

$$\longrightarrow \begin{pmatrix} 2 & 1 & -5 & -2 \\ 0 & 0 & 19 & 9 \\ 0 & 0 & -21 & -7 \end{pmatrix}$$

$\gcd(19,-21) = 1 = 10 \cdot 19 + 9 \cdot (-21)$

$\leadsto U = \begin{pmatrix} 10 & 9 \\ -21 & -19 \end{pmatrix}$

$$\longrightarrow \begin{pmatrix} 2 & 1 & -5 & -2 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & -56 \end{pmatrix}$$

Now, condition 2a holds. But 2b not need this entry to lie in $P(1) = \{0\}$

Can do this with

$$U = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}$$

$$\leadsto \begin{pmatrix} 2 & 1 & 0 & 133 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & -56 \end{pmatrix}$$ this needs to be in $P(-56) = \{0, \dots, 55\}$

Can do this with

$$U = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$\leadsto \begin{pmatrix} 2 & 1 & 0 & 21 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & -56 \end{pmatrix}$$

Now, 2b holds as well. Remains 2c this needs to be in $P = \mathbb{Z}_{\geq 0}$.

Can do this with

$$U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\leadsto \underline{\begin{pmatrix} 2 & 1 & 0 & 21 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & 56 \end{pmatrix}}$$ This is the HNF of A!

<u>Remark</u> 4.7: Coefficients during the computation can get extremely large.
There is an example of a 20x20 integer matrix with entries in $\{0,\dots,10\}$ such that in computation of the HNF integers with up to 1.500 digits arise.
There is a modular version of the algorithm which avoids such problems.

Can similarly define HNF using lower triangular matrices, get this by column operations $A \cdot U$.
Combining the two, we can produce:

<u>Thm</u> 4.8: $A = (a_{ij}) \in Mat_{m \times n}(R)$. Then there are $U \in GL_m(R)$, $V \in GL_n(R)$ such that

$$UAV = \begin{pmatrix} D_r & 0 \\ 0 & 0 \end{pmatrix}$$

where $D_r = \mathrm{diag}(s_1,\dots,s_r)$ with $s_i \neq 0 \ \forall i$ and $s_i \mid s_{i+1} \ \forall i$. The $s_i$ are uniquely determined and are called the <u>elementary divisors</u>. The matrix $UAV$ is called the <u>Smith normal form</u> of $A$.

Again, we illustrate this by an example

$$A = \begin{pmatrix} 4 & 2 & 9 & 5 \\ 6 & 3 & 4 & 3 \\ 8 & 4 & 1 & -1 \end{pmatrix} \overset{HNF}{\rightsquigarrow} \begin{pmatrix} 2 & 1 & 0 & 21 \\ 0 & 0 & 1 & 27 \\ 0 & 0 & 0 & 56 \end{pmatrix} \qquad \gcd(1,27) = 1 = 1 \cdot 1 + 0 \cdot 27$$

Apply $V = \begin{pmatrix} 1 & 0 \\ 27 & -1 \end{pmatrix}$ as column operations:

$$\rightsquigarrow \begin{pmatrix} 2 & 1 & 0 & 21 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 56 \end{pmatrix} \qquad \gcd(1,21) = 1 = 1 \cdot 1 + 0 \cdot 21 \quad \rightsquigarrow \text{apply } V = \begin{pmatrix} 1 & 0 \\ -21 & 1 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 56 \end{pmatrix} \qquad \gcd(2,1) = 1 = 0 \cdot 2 + 1 \cdot 1 \quad \rightsquigarrow \text{apply } V = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 56 \end{pmatrix}$$

Now, change colums

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 56 & 0 \end{pmatrix}$$ The Smith normal form of A
Elementary divisors of A.

Can prove fantastic theorems with this!

Thm 4.9: Let $V$ be a finitely generated $R$-module.
Then
$$V \simeq R^m \oplus \bigoplus_{i=1}^{k} R/(p_i^{m_i})$$
for uniquely determined $m \in \mathbb{N}$, prime elements $p_i$ and uniquely determined $m_i \in \mathbb{N}$.

Proof:
Let $\{v_1, \dots, v_n\}$ be generators of $V$. Let $e_1, \dots, e_n$ be the standard basis vectors of $R^n$. Then $\phi: R^n \longrightarrow V$, $e_i \longmapsto v_i$, is a surjective morphism.
$\leadsto V \simeq R^n / \ker \phi$

$\ker\phi$ is a submodule of a free module, thus free by Thm 3.66. (R PID)
Let $f_1, \dots, f_l$ be a basis of $\ker\phi$. Let $A$ be the matrix of $\ker\phi \hookrightarrow R^n$ in the bases. By Thm 4.8, we can change bases so that

$$A = \begin{pmatrix} D_r & 0 \\ 0 & 0 \end{pmatrix}$$ Smith normal form

Let $D_r = (s_1, \dots, s_r)$. Then it is immediately clear:
$$V \simeq R^n / \ker\phi \simeq R^n / \operatorname{Im} A = \bigoplus_{j=1}^{r} R/(s_j) \oplus \bigoplus_{j=r+1}^{n} R/(0)$$
$$= \bigoplus_{j=1}^{r} R/(s_j) \oplus R^m, \quad m = n-r$$
Now, write $s_j = p_{j1}^{r_{j1}} \cdots p_{jn_j}^{r_{jn_j}}$ with pairwise distinct primes $p_{lk}$

Chinese remainder theorem

$$R/(s_j) \simeq \bigoplus_{k=1}^{n_j} R/(p_{j_k}^{r_{jk}})$$

Now sum all these decompositions. Done.

$\square$

<u>Cor</u>[4.10]: Classification of finitely generated abelian groups $(R=\mathbb{Z})$. $\square$

Another really useful fact:

<u>Cor</u>[4.11]: Let $V$ be a f.g. free $\mathbb{Z}$-module and $U \subseteq V$ a submodule of the same rank. Then $V/U$ is finite and

$[V:U] := |V/U| = |\det(A)|$, where $A$ is the matrix of $U \hookrightarrow V$ in some bases of $U$ and $V$

<u>Proof:</u>

By Smith normal form there are $U, V$ s.t. $UAV = \begin{pmatrix} D_r & \\ & 0 \end{pmatrix}$, Smith normal form, $D_r = \mathrm{diag}(s_1, .., s_r)$.

Then

$$V/U \simeq \bigoplus_{i=1}^{r} \mathbb{Z}/(s_i) \Rightarrow |V/U| = \prod_{i=1}^{r} s_i.$$

Also, since $U, V \in GL(\mathbb{Z}) \rightsquigarrow \det(U), \det(V) = \pm 1$, so

$$|\det(A)| = |\det(U)\det(A)\det(V)| = \prod_{i=1}^{r} s_i.$$

$\square$