The Smith Normal Form using Sage

Morith Hlavaty, Julian Kornweibel

May 20, 2024

1 Definitions

1.1 Definition: Ring

A **Ring** $(R, +, \cdot)$ is a set R with the two operations $+$ (addition) and $\cdot$ (multiplication), for which the following holds true:

- $(R, +)$ is an abelian group under addition, meaning it satisfies all group properties and the commutative property.
- $(R, \cdot)$ is a semigroup under multiplication, meaning it satisfies group properties, but does not require inverse elements or a neutral element.
- The distributive properties apply.

A Ring is called a commutative ring, if it satisfies the commutative property under multiplication.

1.2 Definition: Integral domain

Let R be a Ring. R is a integral domain if it is a nonzero commutative ring in which for each pair of nonzero elements the following property holds true: for $a, b \in R \backslash \{0\}$ is $a * b \neq 0$

1.3 Definition: Ideal

Let I be a subset of a ring $(R, +, \cdot)$. I is an **ideal** if the following holds true:

- $(I, +)$ is a subgroup of $(R, +)$.
- For all $a \in I$ and $r \in R$, $r \cdot a = a \cdot r \in I$

Note also, that we formally differentiate between left- and right-ideal if the ring is not commutative, but we only require a commutative ring for this project. In this case, it is common to write the ideal generated by a as $\langle a \rangle$.
We now define a special type of ideal:

1.4 Definition: Principle Ideal & Principle Ideal Domain (PID)

Let $(R, +, \cdot)$ be a commutative ring. An ideal of the form:

- $a \cdot R = R \cdot a = \{a \cdot r : r \in R\}$

is called a **principle ideal** generated by a.

You can imagine this as a subset of multiples of the elements of the ring over R. The principle ideal generated by $k \in \mathbb{Z}$ is: $k\mathbb{Z} = \{0, \pm k, \pm 2k, ...\}$.

Let $(R, +, \cdot)$ be an integral domain. Then R is a **principle ideal domain** (PID) if every ideal in $(R, +, \cdot)$ is a principle ideal.

1.5 Lemma:

The set of Integers $\mathbb{Z}$ is a PID.

Proof. Let $I \subset \mathbb{Z}$ be an ideal.
Trivially, suppose the $I = \{0\}$
$\Rightarrow I = 0 \cdot \mathbb{Z}$
$\Rightarrow I$ is a principle ideal.
Now let $I \subset \mathbb{Z}$ be a non-zero ideal.
$\Rightarrow$ there exists a smallest positive integer $a \in I$, where $a > 0$.
Now let $b \in I$ and suppose $b > a$. The extended euclidean algorithm for $\mathbb{Z}$ tells us that there must exist $q, r \in \mathbb{Z}$ such that $b = a \cdot q + r$ with $0 \leq r < a$.
$\Rightarrow r = b - a \cdot q$.
Since $a \in I$ and $q \in \mathbb{Z}$,
$\Rightarrow a \cdot q \in I$
$\Rightarrow b - a \cdot q \in I$
$\Rightarrow r \in \mathbb{Z}$.
And since a is the smallest possible integer in I
$\Rightarrow r = 0$
$\Rightarrow$ ever element in I must be of the form $b = a \cdot q$
$\Rightarrow I = a \cdot \mathbb{Z}$. Meaning I is a principle ideal.
$\Rightarrow$ Every ideal in $\mathbb{Z}$ is a principle ideal, so $\mathbb{Z}$ is a PID.

□

1.6 Lemma:

every Field $\mathbb{F}$ is a PID

Proof. Let F be a field and $I \subset F$ be a non-zero ideal (as the zero case is identical

to the one above).
$\Rightarrow 1 = a^{-1} \cdot a \in I$, where a^{-1} exists since F is a field and $a \neq 0$.
$\Rightarrow \forall b \in F,\ b = b \cdot 1 \in I$
$\Rightarrow I = F = \langle 1 \rangle$ if $I \neq \{0\}$
$\Rightarrow$ The only ideals of a field F are $\langle 0 \rangle = \{0\}$ and $\langle 1 \rangle = F$, both of which are clearly principal ideals.

□

1.7 Definition: Identity Matrix

An $n \times n$ matrix I_n is the **identity matrix** if all the diagonal elements are equal to 1 and all the other elements are zero, meaning it is of the form:

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}$$

1.8 Definition: Invertible Matrix

A matrix P over a PID is **invertable** if there exists a matrix Q over the PID such that:

- $P \cdot Q = I_n$

Clearly, if P and Q are units, then PQ is also a unit.

1.9 Definition: Elementary Matrix

There eixist three types of elementary matricies defined as followed:
A $n \times n$ matrix E_i^α in the form:

$$\begin{bmatrix} 1 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & & \vdots \\ \vdots & & \ddots & \alpha & \ddots & & \vdots \\ \vdots & & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 & 1 \end{bmatrix}$$

with α some value in the PID.
This represents multiplication of a row or column by α and is invertable.
A $n \times n$ matrix $E_{i,j}^\alpha$ in the form:

$$\begin{bmatrix} 1 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & 1 & \ddots & \alpha & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 & 1 \end{bmatrix}$$

with α some value in the PID.
This represents adding a multiple of a row or column and is invertable by appling the matrix with -α

1.9 Definition: Elementary Matrix

A $n \times n$ matrix $E_{i,j}$ in the form:

$$\begin{bmatrix} 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & & & & \vdots \\ \vdots & & \ddots & 0 & \ddots & 1 & & & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & & & \vdots \\ \vdots & & & 1 & \ddots & 0 & \ddots & & \vdots \\ \vdots & & & & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 \end{bmatrix}$$

This represents swapping two rows or columns and is invertable by applying the same matrix again

2 Smith Normal Form

2.1 Definition Smith Normal Form (SNF)

Let A be a non-zero $m \times n$ matrix over a PID R.
There exist **invertable** $m \times m$ and matrices P and Q over R such that the product $P \cdot A \cdot Q$ is of the form:

$$PAQ = \begin{bmatrix} \alpha_1 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & \alpha_2 & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ \vdots & & \ddots & \alpha_r & \ddots & & \vdots \\ \vdots & & & \ddots & 0 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 & 0 \end{bmatrix} = S$$

which has the following attributes:

- the diagonal elements α_i satisfy: $\alpha_i \mid \alpha_{i+1}$ for all i, where $1 \leq i < r$.
- P is a product of elementary row matrices.
- Q is a product of elementary column matrices.

$S = PAQ$ is the **Smith normal form** of A.

2.2 Algorithm

The algorithm will be presented in the 'Jupyter Notebook', but the basic idea will always be the following:
Let A, P, Q, and S be defined as they were in **2.1**, then:

$$\begin{bmatrix} A & I_m \\ I_n & * \end{bmatrix} \longrightarrow \begin{bmatrix} S & P \\ Q & * \end{bmatrix}$$

which we can always obtain by applying elementary row and column operations.