## 1. Some background

A ring $R$ is a set on which the operations of addition, subtraction and multiplication are defined. Moreover, we also have an element 1 which is a multiplicative identity. (Subtraction means that we must have 0 which is an additive identity.) We will work with rings $R$ in which $ab = ba$; these are called commutative rings. If you do not know any sophisticated rings then you can think of the ring $\mathbf{Z}$ of integers.

One way to create a new ring is to consider the set $M_n(R)$ of $n \times n$ matrices with entries in the ring $R$. We can define multiplication and addition of matrices in the usual way. This is a very fruitful way of creating new rings from old and has paved the way for most of the algebra of the 20th century.

However, today we will look at a different approach. Given matrices $A$ and $B$ which are possibly of *different sizes*, we define $A \oplus B$ as the block matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. We can also define $A \otimes B$ as the block matrix

$$\begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1p}B \\ a_{21}B & a_{22}B & \dots & a_{1p}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{p1}B & a_{p2}B & \dots & a_{pp}B \end{pmatrix}$$

Note that $A \oplus B$ is *not* (in general) the same as $B \oplus A$ and so on. How do we make these operations into "proper" addition and multiplication operations?

We note that the characteristic polynomial of $A \oplus B$ is the *product* of the characteristic polynomial of $A$ and the characteristic polynomial of $B$. Is there a way to understand the characteristic polynomial of $A \otimes B$ in a similar way?

Consider the polynomial $\det(1 - At)$ for some variable $t$. We note a very important fact:

> The coefficients of the characteristic polynomial of a matrix are the values of a *universal* polynomial in the entries of the matrix.

The polynomial is "universal" in the sense that it does not depend on the coefficients of the matrix but only on its size.

Given any polynomial $P(t)$ of the form $1 + s_1 t + \dots s_p t^p$, Cayley showed how we can write a matrix $A_P$ for which $\det(1 - At) = P(t)$. So we could *define* addition and multiplication of such polynomials by declaring

$$\begin{aligned} P \oplus Q &= \det(1 - (A_P \oplus A_Q)t) \\ P \otimes Q &= \det(1 - (A_P \otimes A_Q)t) \end{aligned}$$

Written this way it becomes obvious that:

> The coefficients of $P \oplus Q$ and $P \otimes Q$ are the values of universal polynomials applied to the coefficients of $P$ and $Q$.

Can we further clarify these operations in any way?

### 1.1. Some heuristic calculations.

If $A$ is diagonalisable with distinct eigenvalues $a_i$, we can write

$$\det(1 - At) = \prod(1 - a_i t)$$

Note that the right-hand side can be expanded as

$$\prod(1 - a_i t) = 1 - s_1 t + s_2 t^2 + \dots + (-1)^p s_p t^p$$

where

$$\begin{aligned} s_1 &= a_1 + \cdots + a_p \\ s_2 &= a_1a_2 + a_1a_3 + \cdots + a_1a_p + a_2a_3 + \cdots + a_{p-1}a_p \\ s_3 &= a_1a_2a_3 + \dots \end{aligned}$$

and so on (each $s_k$ is the sum of the products of $k$ *distinct* $a_i$'s). These are called the elementary symmetric functions of the eigenvalues of the matrix since:

(1) The $s_k$ do not change if we permute the order in which we write the roots.
(2) Every function of $(a_1, \dots, a_p)$ that does not change when we permute the $a_i$'s is actually a function of $(s_1, \dots, s_p)$.

This shows us an important fact:

> The symmetric functions in the eigenvalues of a matrix are *universal* polynomials in the entries of the matrix.

In particular, we can determine these symmetric functions *without* calculating the eigenvalues of the matrix.

The product expression above has an important formal consequence. Formally, we have

$$-\log(1-at) = \sum_{k\geq 1}(at)^k/k$$

which gives

$$-t\frac{d}{dt}\log(1-at) = \sum_{k\geq 1} a^k t^t$$

Adding up the expressions for the various $a_i$'s we obtain

$$g_A(t) = -t\frac{d}{dt}\log\det(1-At) == \sum_i -t\frac{d}{dt}\log(1-a_it) = \sum_{k\geq 1}\left(\sum_i a_i^k\right)t^k$$

The expressions $N_k = \sum_i a_i^k$ are called the Newton polynomials of the eigenvalues (since Newton first worked with them). Expanding the *left* hand side formally using $-\log(1-x) = \sum_{i\geq 1} x^i/i$ we can obtain an expression of the Newton polynomials in terms of the symmetric polynomials.

The reason for this long calculation is to note the following formulae. Let us write

$$g_A(t) = \sum_i N_i(A)t^i \text{ and } g_B(t) = \sum_i N_i(B)t^i$$

Then we have

$$\begin{aligned} g_{A\oplus B}(t) &= \sum_i (N_i(A) + N_i(B))\, t^i \\ g_{A\otimes B}(t) &= \sum_i (N_i(A)\cdot N_i(B))\, t^i \end{aligned}$$

In particular, *at some level* we are doing ordinary addition and multiplication!

## 2. Lambda of a ring

With the above background, we can define $\Lambda_+(R)$ to be the collection of all polynomials with coefficients in $R$ such that the constant term is 1. Let $P \mapsto A_P$ denote the map that associates a polynomial of degree $p$ to its $p \times p$ companion matrix:

$$P = 1 + s_1 t + s_2 t^2 + \cdots + s_p t^p \mapsto A_P = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_p & s_{p-1} & s_{p-2} & \ldots & s_1 \end{pmatrix}$$

In that case, $P = \det(1 + A_P t)$. Given $P$ and $Q$ in $\Lambda_+(R)$ we define define addition and multiplication

$$\begin{aligned} P \oplus Q &= \det\left(1 + (A_P \oplus A_Q)t\right) \\ P \otimes Q &= \det\left(1 + (A_P \otimes A_Q)t\right) \end{aligned}$$

Note that

$$\det(1 + At) = \det\big(1 + (G^{-1}AG)t\big)$$

Using this and suitable choices of $G$ one can show that these operations are commutative and associative. Moreover $\otimes$ distributes over $\oplus$. The constant polynomial 1 acts as identity for $\oplus$ and the polynomial $(1+t)$ acts as identity for $\otimes$.

One important point to note is that the coefficients of $t^k$ in $P \oplus Q$ or $P \otimes Q$ *do not* depend on the coefficients of $t^l$ in $P$ or $Q$ when $l > k$.

Let $\Lambda_n(R)$ denotes the collection of all polynomials of degree at most $n$ which have constant term $n$. We define $\oplus$ and $\otimes$ as above except that we ignore all terms in the expressions that involve $t^k$ for $k > n$. As a result of the above point, we note that this way of ignoring higher order terms does not change the formulas for the coefficients of powers of $t$ in $P \oplus Q$ or $P \otimes Q$.

In the opposite direction one can define $\Lambda(R)$ to be the collection of all (formal) power series of the form $P = 1 + \sum_{k=1}^{\infty} s_k t^k$. There is a natural map $\Lambda(R) \to \Lambda_n(R)$ called *truncation* that restricts to the first $n+1$ terms of the power series. By what has been said above, the operations $\oplus$ and $\otimes$ extend to $\Lambda(R)$. In addition, we have "subtraction". The formal power series as above has the formal inverse

$$(1 + \sum_{k=1}^{\infty} s_k t^k)^{-1} = 1 - (\sum_{k=1}^{\infty} s_k t^k) + (\sum_{k=1}^{\infty} s_k t^k)^2 + \ldots$$

By expanding these we see that the coefficient of $t^k$ is a universal polynomial in $(s_1, \ldots, s_k)$; in other words, it does not involve $s_l$ for $l > k$. We define $\ominus P$ as the right-hand side.

## 3. Witt ring

A slightly different approach is to consider the collection $W(R)$ of all product series of the form

$$P = \prod_{k=1}^{\infty} (1 - w_k t^k)$$

Let

$$P = \sum_{k=1}^{\infty} s_k t^k$$

denote the expansion of the right-hand side. We can see that

$$s_k = w_k + U_k(w_1, \ldots, w_{k-1})$$

Note that $w_1 = s_1$. Hence, by induction, this means that there are universal polynomials $V_k$ so that

$$w_k = s_k + V_k(s_1, \ldots, s_{k-1})$$

It follows that the association $(w_1, \ldots, w_k) \mapsto (s_1, \ldots, s_k)$ is one-to-one and onto. In other words, $W(R)$ is in fact in bijection with $\Lambda(R)$.

We thus see that $W(R)$ is closed under the operations $\oplus$ and $\otimes$. We note that the product ($\otimes$) of elements of $W(R)$ has the nice formula

$$\prod_{k\geq 1}(1 - x_k t^k) \otimes \prod_{l\geq 1}(1 - y_l t^l) = \prod_{l,k\geq 1 h=\gcd(k,l)} (1 - x_k^{l/h} y_l^{k/h})^h$$

The isomorphism given above between $W(R)$ and $\Lambda(R)$ allows us to interchange between the two.

3.1. **Witt's ghosts.** We can give a heuristic reason for this as follows. Assume that each $w_n$ has an $n$-th root $w_n^{1/n}$ and that $\zeta_n$ is a primitive $n$-th root of unity. We can then write

$$P = \prod_{k=1}^{\infty} \prod_{i=0}^{k-1} (1 - w_k^{1/k} \zeta_k^i t)$$

We then get

$$-t\frac{d}{dt}\log P = \sum_{n=1}^{\infty} \left( \sum_{k=1}^{\infty} \left( \sum_{i=0}^{k-1} w_k^{n/k} \zeta_k^{ni} \right) \right) t^n$$

We use the "cancellation of characters" which says

$$\sum_{i=0}^{k-1} \zeta_k^{ni} = \begin{cases} 0 & k \text{ does not divide } n \\ k & n = kd \end{cases}$$

The above expression then simplifies to

$$-t\frac{d}{dt}\log P = \sum_{n=1}^{\infty} \left( \sum_{k|n} k w_k^{n/k} \right) t^n$$

The terms

$$w^{(n)} = \sum_{k|n} k w_k^{n/k}$$

are called Witt's ghost components. As noted above, the formulae for $\oplus$ and $\otimes$ can be viewed as addition and multiplication of the ghost components.