THE ALGEBRA OF PARTITIONS

ANDREW HUBERY

This is a fleshed-out version of my talk, so including a brief section on existence of Hall polynomials and how that follows from Green's Formula which is coming next, and also a little more on Macdonald's ring of symmetric functions. The main references are

I.G. Macdonald, Symmetric functions and Hall polynomials (2nd ed.), Oxford Math. Monographs, Oxford Univ. Press.

A Hubery, Ringel-Hall algebras of cyclic quivers, São Paulo Journal of Math. Sciences 4 (2010), 351–398.

1. Discrete valuation rings

Let R be a DVR with finite residue field $k = \mathbb{F}_q$ and maximal ideal (π). For example we could take $k[[t]]$ or $\mathbb{Z}_p$.

Let $\operatorname{mod} R$ be the category of finite length R-modules. The indecomposables are of the form $S_m := R/(\pi^m)$ for $m \geq 1$, and the unique simple is $S = S_1 = k$. Moreover, each indecomposable has a unique composition series

$$0 \subset S \subset S_2 \subset \cdots \subset S_m, \quad S_i = (\pi^{m-i}) \subset R,$$

so $\operatorname{mod} R$ is a uniserial category.

The Grothendieck group is simply $\mathbb{Z}$, where the class of S_m is just its length $m = \ell_R(S_m)$.

1.1. Hom and ext.

In the category $\operatorname{Mod} R$ of all R-modules we have a projective presentation

$$0 \to R \xrightarrow{\pi^m} R \to S_m \to 0.$$

Hence applying $\operatorname{Hom}(-, X)$ for a module X, and using that $\operatorname{Hom}(R, X) \cong X$, we have the four term exact sequence

$$0 \to \operatorname{Hom}(S_m, X) \to X \xrightarrow{\pi^m} X \to \operatorname{Ext}^1(S_m, X) \to 0.$$

Thus

$$\operatorname{Hom}(S_m, X) \cong \operatorname{soc}^m X = \operatorname{Ker}(\pi^m) \quad \text{and} \quad \operatorname{Ext}^1(S_m, X) \cong X/\pi^m X = \operatorname{Coker}(\pi^m).$$

Moreover

$$\operatorname{Ext}^i(S_m, X) = 0 \quad \text{for all } i \geq 2,$$

so the category $\operatorname{mod} R$ is hereditary.

Moreover, the Euler form vanishes identically:

$$\begin{aligned}\langle S_m, X\rangle &:= \sum_i (-1)^i \ell_R(\operatorname{Ext}^i(S_m, X)) \\ &= \ell_R(\operatorname{Hom}(S_m, X)) - \ell_R(\operatorname{Ext}^1(S_m, X)) = \ell_R(X) - \ell_R(X) = 0.\end{aligned}$$

1.2. **Duality.** Consider the Prüfer module E in $\operatorname{Mod} R$, given by

$$E := \varinjlim S_m.$$

Then the functor

$$D := \operatorname{Hom}(-, E)$$

induces a duality on $\operatorname{mod} R$ such that $D(X) \cong X$.

Note that when R contains a coefficient field, so is a k-algebra, then we can instead consider the vector space duality $D = \operatorname{Hom}_k(-, k)$.

Now, applying $\operatorname{Hom}(X, -)$ for $X \in \operatorname{mod} R$ to the injective presentation

$$0 \to S_m \to E \xrightarrow{\pi^m} E \to 0,$$

we get the four term exact sequence

$$0 \to \operatorname{Hom}(X, S_m) \to D(X) \xrightarrow{\pi^m} D(X) \to \operatorname{Ext}^1(S_m, X) \to 0.$$

Since multiplication by π^m on $D(X)$ is the dual of multiplication by π^m on X we obtain

$$\operatorname{Hom}(X, S_m) \cong \operatorname{soc}^m D(X) \cong D(\operatorname{Ext}^1(S_m, X)).$$

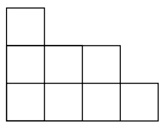
2. The algebra of partitions

By the Krull-Remak-Schmidt Theorem, every R-module is a finite direct sum of indecomposables, unique up to reordering. Thus the isomorphism classes of R-modules are in bijection with partitions $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots)$ via

$$S_\lambda := S_{\lambda_1} \oplus S_{\lambda_2} \oplus \cdots$$

Note that $\ell(S_\lambda) = |\lambda| = \sum_i \lambda_i$.

A useful mental image is to regard the indecomposable S_m as a tower of height m, with the generator at the top. This is appropriate here since the S_m are uniserial. Then S_λ is a city skyline, consisting of towers for each indecomposable summand, and so we have reconstructed the Young diagram (or its reflection in maybe the more standard convention). For example, taking $\lambda = (3, 2, 2, 1)$ we would draw this as

$\lambda = (3, 2, 2, 1)$ 

The (Ringel-)Hall algebra of $\operatorname{mod} R$ therefore has basis indexed by partitions

$$H = \bigoplus_\lambda \mathbb{Q} u_\lambda$$

and is $\mathbb{Z}$-graded, where $\deg u_\lambda = |\lambda|$.

2.1. **Some computations.** (1) As an R-module we have $\operatorname{Hom}(S_a, S_b) \cong S_d$, where $d = \min\{a, b\}$. Hence also $\operatorname{Ext}^1(S_a, S_b) \cong S_d$. It follows that for all partitions λ, μ we have

$$|\operatorname{Hom}(S_\lambda, S_\mu)| = |\operatorname{Ext}^1(S_\lambda, S_\mu)| = q^{d_{\lambda\mu}}, \quad \text{where} \quad d_{\lambda,\mu} := \sum_{i,j} \min\{\lambda_i, \mu_j\}.$$

Let λ' denote the conjugate partition to λ, so given by reflecting the Young diagram in the line $x = y$. Then

$$d_{\lambda,\mu} = \sum_i \lambda'_i \mu'_i.$$

We have two binary opertaions on partitions, namely addition and union

$$\lambda + \mu = (\lambda_1 + \mu_1, \lambda_2 + \mu_2, \ldots) \quad \text{and} \quad \lambda \cup \mu = (\lambda_1, \mu_1, \lambda_2, \mu_2, \ldots),$$

but where we may have to rearrange the parts of $\lambda \cup \mu$ into decreasing order. Note that $\lambda' + \mu' = (\lambda \cup \mu)'$, so these operations are conjugate. It follows that we can regard $d_{\lambda,\mu}$ as an inner product on partitions with respect to the union operation. This yields the quadratic form $n(\lambda)$, where

$$d_{\lambda,\lambda} = |\lambda| + 2n(\lambda), \quad n(\lambda) = \sum_i \tbinom{\lambda'_i}{2}.$$

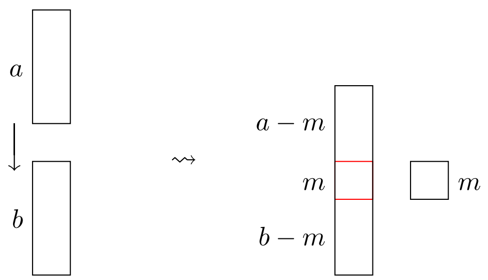
(2) As a ring we have $\mathrm{End}(S_a) \cong R/(\pi^a)$. Thus endomorphisms of S_a^r can be regarded as matrices of size r over $R/(\pi^a)$. Using the canonical epimorphism $S_a \twoheadrightarrow S$, with kernel S_{a-1}, we get a surjective group homomorphism

$$\mathrm{Aut}(S_a^r) \twoheadrightarrow \mathrm{Aut}(S^r) \cong \mathrm{GL}_r(k)$$

having kernel those matrices of size r over $\mathrm{End}(S_{a-1}) \cong R/(\pi^{a-1})$. It follows that

$$|\mathrm{Aut}(S_a^r)| = q^{ar^2}(1-q^{-1})(1-q^{-2})\cdots(1-q^{-r}).$$

(3) We next compute $u_{(a)}u_{(b)}$ in the Hall algebra. From our mental picture, we need to stack a tower of height a on top of a tower of height b, but if we use too much force, then m floors of the towers will get squashed, and therefore need to be replaced.



This suggest we get an extension with middle term corresponding to the partition $(a+b-m, m)$ for each $0 \le m \le d := \min\{a, b\}$.

For $m = 0$ the middle term is S_{a+b}, so indecomposable and uniserial, so $F^{(a+b)}_{(a)(b)} = 1$.

For $0 < m < d$ we want a submodule $U \le S_{a+b-m} \oplus S_m$ such that $U \cong S_b$. The generator of U must therefore be (π^{a-m}, x) (up to a unit of R). We also need the quotient to be isomorphic to S_a, but if $x \in \pi S_m$, then the quotient will need two generators. Thus $x \in S_m \setminus \pi S_m$. We therefore get $F^{(a+b-m,m)}_{(a)(b)} = q^m(1-q^{-1})$.

For $m = d$ but $a \neq b$ we want a submodule $U \le S_a \oplus S_b$ with $U \cong S_b$ and the quotient isomorphic to S_a. Since $S_a \ncong S_b$ the generator for U must be $(x, 1)$ for some $x \in S_a$ with $\pi^b x = 0$. Thus $F^{(a,b)}_{(a)(b)} = q^d$.

Finally, for $m = d = a = b$ we want a submodule $U \le S_a^2$ with $U \cong S_a$ (and then necessarily the quotient will be isomorphic to S_a). Here we can take as the generator $(x, 1)$ for any $x \in S_a$, or $(1, y)$ for anty $y \in \pi S_a$ (to avoid repetition). Hence $F^{(a,a)}_{(a)(a)} = q^a(1+q^{-1})$.

Using Riedtmann's Formula

$$F^X_{MN} = \frac{|\mathrm{Ext}^1(M,N)_X|}{|\mathrm{Hom}(M,N)|} \times \frac{|\mathrm{Aut}(X)|}{|\mathrm{Aut}(M)||\mathrm{Aut}(N)|},$$

we can compute

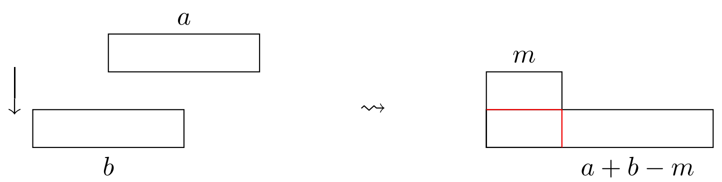
$$|\mathrm{Ext}^1(S_a,S_b)_{S_{(a+b-m,m)}}| = \begin{cases} q^{d-m}(1-q^{-1}) & \text{for } 0 \le m < d; \\ 1 & \text{for } m = d. \end{cases}.$$

Suming over m reveals that we have indeed accounted for all possible extensions

$$\sum_m |\operatorname{Ext}^1(S_a, S_b))_{S_{(a+b-m,m)}}| = q^d = |\operatorname{Ext}^1(S_a, S_b)|.$$

(4) At the other extreme we can compute extensions between semisimple modules, so $u_{(1^a)}u_{(1^b)}$.

Here we want to place a row of a blocks on top of a row of b blocks, and again they may overlap by m blocks for $0 \le m \le d := \min\{a, b\}$.



This suggest we get an extension with middle term corresponding to the partition $(2^m 1^{a+b-2m})$ for each $0 \le m \le d$.

For the Hall number, we need to take a submodule of the socle of length b, whose quotient is again semisimple. We must therefore take the whole of the socle of each indecomposable S_2, and then choose a submodule of S^{a+b-2m} of length $b-m$. Thus

$$F^{(2^m 1^{a+b-2m})}_{(1^a)(1^b)} = \left|\operatorname{Gr}\binom{a+b-2m}{b-m}(k)\right| = \begin{bmatrix} a+b-2m \\ b-m \end{bmatrix}_q$$

where $\begin{bmatrix} n \\ m \end{bmatrix}_q$ is the quantum binomial coefficient, so

$$[n]_q := \frac{q^n - 1}{q-1}, \quad [n]_q! := [n]_q \cdots [2]_q[1]_q, \quad \begin{bmatrix} n \\ m \end{bmatrix}_q := \frac{[n]_q!}{[m]_q![n-m]_q!}.$$

Again, using Riedtmann's Formula, we have

$$|\operatorname{Ext}^1(S^a, S^b)_{S_2^m \oplus S_1^{a+b-2m}}| = \begin{bmatrix} a \\ m \end{bmatrix}_q \begin{bmatrix} b \\ m \end{bmatrix}_q |\operatorname{GL}_m(k)|.$$

Summing over m yields the quantum binomial identity

$$\sum_m \begin{bmatrix} a \\ m \end{bmatrix}_q \begin{bmatrix} b \\ m \end{bmatrix}_q |\operatorname{GL}_m(k)| = q^{ab},$$

an identity which has no obvious classical analogue (since if we set $q = 0$ then almost all terms on the left vanish).

(5) Using the duality $D = \operatorname{Hom}(-, E)$ we see that $F^\nu_{\lambda\mu} = F^\nu_{\mu\lambda}$, and hence that H is a commutative algebra, and a cocommutative coalgebra.

3. The algebra structure

We introduce the dominance partial order on partitions, so for two partitions λ and μ of the same size

$$\lambda \le \mu \quad \text{provided} \quad \lambda_1 + \cdots + \lambda_i \le \mu_1 + \cdots + \mu_i \text{ for all } i.$$

Note that $\lambda \le \mu$ if and only if $\lambda' \ge \mu'$.

Lemma 3.1. *If the Hall number $F^\nu_{\lambda\mu}$ is non-zero, then $\lambda \cup \mu \le \nu \le \lambda + \mu$ in the dominance ordering. Moreover, the Hall number is always non-zero for $\nu = \lambda \cup \mu$.*

Proof. Suppose we have a short exact sequence

$$0 \to S_\mu \xrightarrow{f} S_\nu \xrightarrow{g} S_\lambda \to 0.$$

Note that if $U \leq S_\nu$ is any submodule, then we obtain a short exact sequence

$$0 \to f^{-1}(U) \to U \to g(U) \to 0.$$

For the first inequality note that the length of $\mathrm{soc}^i(S_\lambda)$ is $\lambda'_1 + \cdots + \lambda'_i$. In our mental picture, we are just taking the bottom i floors of our tower blocks.

Now, clearly g sends everything in $\mathrm{soc}^i(S_\nu) = \mathrm{Ker}(\pi^i)$ to $\mathrm{soc}^i(S_\lambda)$, and similarly $f^{-1}(\mathrm{soc}^i(S_\nu)) \subset \mathrm{soc}^i(S_\mu)$. We deduce that

$$\nu'_1 + \cdots + \nu'_i \leq \lambda'_1 + \mu'_1 + \cdots + \lambda'_i + \mu'_i,$$

so that $\nu' \leq \lambda' + \mu'$, and hence $\nu \geq \lambda \cup \mu$.

If instead we consider $S_\nu^{(\leq i)} = S_{\nu_1} \oplus \cdots \oplus S_{\nu_i}$, so the tallest i towers, then its image under g requires at most i generators, so its length is at most that of $S_\lambda^{(\leq i)}$. Similarly if we intersect this with $f(S_\mu)$ then it can again have at most i indecomposable summands, and so its length is bounded by that of $S_\mu^{(\leq i)}$. Thus

$$\nu_1 + \cdots + \nu_i \leq \lambda_1 + \mu_1 + \cdots + \lambda_i + \mu_i,$$

so that $\nu \leq \lambda + \mu$.

Finally, if $\nu = \lambda \cup \mu$, then $S_\nu \cong S_\lambda \oplus \S_\mu$, and so we have the split exact sequence. Using Riedtmann's Formula, and noting that $|\,\mathrm{Ext}^1(S_\lambda, S_\mu)_{S_{\lambda\cup\mu}}| = 1$, we see that the Hall number in this case is non-zero. □

With a little bit more work we can also prove some other necessary conditions for extensions to exist; for example, we must have $\nu_i \geq \max\{\lambda_i, \mu_i\}$ for all i, usually written $\nu \supset \lambda, \mu$. The following example shows that these conditions are insufficient.

Set $\lambda = (2)$, $\mu = (1,1)$ and $\nu = (2,2)$ we see that $\lambda \cup \mu = (2,1,1) \leq \nu \leq (3,1) = \lambda + \mu$, and also $\lambda, \mu \subset \nu$. On the other hand, S_ν is not an extension of S_λ by S_μ. To see this, note that there is essentially only one epimorphism $g\colon S_\nu = S_2^2 \twoheadrightarrow S^2 = S_\mu$, and its kernel is the socle S^2 and not $S_\lambda = S_2$.

In fact, it is an open problem to describe precisely when an extension exists (see later).

Theorem 3.2. *The $u_{(a)}$ corresponding to the indecomposable modules are algebraically independent in H and generate H. Thus*

$$H = \mathbb{Q}[u_{(1)}, u_{(2)}, u_{(3)}, \ldots]$$

is a polynomial ring on countable many generators.

Proof. For a fixed n we know that the graded piece H_m has basis the u_λ for partitions λ of size m. Set $x_\lambda := u_{(\lambda_1)} u_{\lambda_2} \cdots$. These again have degree m, and so we can form the matrix expressing the x_λ in terms of the u_λ. This has coefficients given by the iterated Hall numbers $F^\mu_{\lambda_1\lambda_2\cdots}$, since

$$x_\lambda = \sum_\mu F^\mu_{\lambda_1\lambda_2\cdots} u_\mu.$$

By repeated use of the previous lemma we see that these Hall numbers are non-zero only for μ in the range

$$\lambda_1 \cup \lambda_2 \cup \cdots = \lambda \leq \mu \leq m = \lambda_1 + \lambda_2 + \cdots .$$

Moreover, the Hall number for $\mu = \lambda$ is non-zero. Thus, if we arrange the rows and columns of the matrix with respect to the dominance ordering, then the matrix will be upper triangular with non-zero entries on the diagonal. Thus the x_λ also form a basis for H_n, as required. □

4. Hopf algebra structure

We will see in the next lecture (on Green's Formula) that the Hall algebra is in fact a Hopf algebra. Moreover, the inner product given by

$$\{u_\lambda, u_\mu\} := \delta_{\lambda\mu}\frac{q^{|\lambda|}}{|\operatorname{Aut}(S_\lambda)|}$$

is a Hopf pairing, so in particular

$$\{xy, z\} = \{x\otimes y, \Delta(z)\} = \sum\{x,z'\}\{y,z''\}, \quad \text{where } \Delta(z) = \sum z'\otimes z''.$$

Since the S_m are uniserial, every submodule and quotient module is again indecomposable, and hence

$$\Delta(u_{(m)}) = \sum_{a+b=m}\frac{|\operatorname{Aut}(S_m)|}{|\operatorname{Aut}(S_a)||\operatorname{Aut}(S_b)|}u_{(a)}\otimes u_{(b)}.$$

If we therefore set

$$c_0 := 1, \quad c_m := (1-q^{-1})u_{(m)} \quad \text{for } m\geq 1,$$

then

$$H = \mathbb{Q}[c_1,c_2,c_3,\dots] \quad \text{and} \quad \Delta(c_m) = \sum_{a+b=m} c_a\otimes c_b.$$

Moreover,

$$\{c_m, c_n\} = \delta_{mn}(1-q^{-1}).$$

4.1. **Primitive elements.** There are actually many such generators for H satisfying the same comultiplication rule, but we can get a canonical choice of generators by finding primitive elements, so elements p_m of degree m such that $\Delta(p_m) = p_m\otimes 1 + 1\otimes p_m$.

The easiest way to do this is via generating functions.

Proposition 4.1. *Suppose we have a commutative Hopf algebra H, and elements x_m, y_m for $m\geq 1$. We also set $x_0 = 1$. Form the generating functions*

$$X(T) := \sum_{m\geq 0} x_m T^m \quad \textit{and} \quad Y(T) := \sum_{m\geq 1} y_m T^{m-1}.$$

Suppose that $Y(T) = \frac{d}{dT}\log X(T)$, equivalently $X(T)Y(T) = \frac{d}{dT}X(T)$, or in terms of the elements themselves

$$mx_m = \sum_{a=1}^{m} y_a x_{m-a}.$$

Then

$$\Delta(x_m) = \sum_{a+b=m} x_a\otimes x_b \quad \textit{if and only if} \quad \Delta(y_m) = y_m\otimes 1 + 1\otimes y_m.$$

Moreover, under these conditions, if we have a symmetric Hopf pairing $\{-,-\}$ on H, then $\bar{Y}(T) = \frac{d}{dT}\log\bar{X}(T)$, where

$$\bar{X}(T) := \sum_{m\geq 0}\{x_m, x_m\}T^m \quad \textit{and} \quad \bar{Y}(T) = \sum_{m\geq 1}\tfrac{1}{m}\{y_m, y_m\}T^{m-1}.$$

Theorem 4.2. *In the Hall algebra H set*

$$p_m := \sum_{|\lambda|=m}(1-q)(1-q^2)\cdots(1-q^{\ell(\lambda)-1})u_\lambda,$$

where $\ell(\lambda)$ is the length of the partition, so the number of non-zero parts.

Then the p_m are primitive and generate H, and $\{p_m, p_n\} = \delta_{mn}m/(1-q^{-m})$.

Sketch. The idea is to apply the previous proposition, using $x_m = c_m$ and $y_m = (1 - q^{-m})p_m$. We therefore just need to show that

$$mx_m - y_m = \sum_{0<a<m} y_a x_{m-a}.$$

The idea is now to use the observation that $\sum_\lambda F^{\mu}_{\lambda(a)}$ equals the number of injective maps from S_a to S_μ, divided out by $|\operatorname{Aut}(S_a)|$, and a map is injective provided it does not factor through the canonical epimorphism $S_a \twoheadrightarrow S_{a-1}$. Also, given such an injective map, say with cokernel S_λ, then $\ell(\lambda) = \ell(\mu)$ unless the extension was split.

In particular, we do not need to do any actual computations of Hall numbers. □

Corollary 4.3. *For a partition $\lambda = (1^{m_1}2^{m_2}\cdots)$ set*

$$z_\lambda(t) := \prod_r \Big(m_r!\Big(\frac{r}{1-q^{-r}}\Big)^{m_r}\Big).$$

Then, writing $p_\lambda := p_{\lambda_1}p_{\lambda_2}\cdots = p_1^{m_1}p_2^{m_2}\cdots$ as usual, these form a basis for the Hall algebra H and

$$\{p_\lambda, p_\mu\} = \delta_{\lambda\mu} z_\lambda(q^{-1}).$$

Proof. We know that the p_m generate H, and so by computing the dimensions of each graded piece H_m we know that the p_λ form a basis for H. The formula for their inner product now follows by induction, using that tha p_m are primitive. □

5. Hall polynomials

Recall that the isomorphism classes of finite length R-modules are indexed by partitions, and is therefore independent of R.

We have also seen in §2.1 (1) that $|\operatorname{Hom}(S_\lambda, S_\mu)| = q^{d_{\lambda,\mu}}$, where q is the size of the residue field k and $d_{\lambda,\mu}$ is an integer depending only on the partitions. We can interpret this as saying there is a polynomial $h_{\lambda,\mu}(t) \in \mathbb{Z}[t]$ (namely $h_{\lambda,\mu} = t^{d_{\lambda,\mu}}$) such that, for any R with finite residue field $k = \mathbb{F}_q$, we have $|\operatorname{Hom}(S_\lambda, S_\mu))| = h_{\lambda,\mu}(q)$. In other words, there exists a universal polynomial giving the sizes of the homomorphism groups.

Extending the example in §2.1 (2), we see that there is also a universal polynomial $a_\lambda(t) \in \mathbb{Z}[t]$ giving the sizes of the automorphism groups, so for any R with finite residue field $k = \mathbb{F}_q$ we have $|\operatorname{Aut}(S_\lambda)| = a_\lambda(q)$. Explicitly we have

$$a_\lambda(t) = t^{d_{\lambda,\lambda}} \prod_r (1-t^{-1})(1-t^{-2})\cdots(1-t^{-m_r}) \quad \text{for} \quad \lambda = (1^{m_1}2^{m_2}3^{m_3}\cdots).$$

Note that $a_\lambda(t)$ is a monic polynomial in u.

Lemma 5.1. *Suppose we have a function $f = p/a$ such that $p, a \in \mathbb{Z}[t]$ and a is monic. If $f(q) \in \mathbb{Z}$ for infinitely many $q \in \mathbb{Z}$, then $f \in \mathbb{Z}[t]$.*

Proof. Since a is monic we can write $f = g + h/a$ where $g \in \mathbb{Z}[t]$ and $e = \deg(h) < \deg(a) = d$. Then we can find a positive rational number c such that $|h(q)/a(q)| < c/q^{d-e}$ for all integers q sufficiently large. Since $f(q) \in \mathbb{Z}$ for infinitely many such q, we must have $h(q) = 0$ and hence $f = g \in \mathbb{Z}[t]$. □

Theorem 5.2. *There is a universal polynomial $f^\nu_{\lambda\mu}(t) \in \mathbb{Z}[t]$ giving the sizes of the Hall numbers $F^\nu_{\lambda\mu}$, so for any R with finite residue field $k = \mathbb{F}_q$ we have $F^\nu_{\lambda\mu} = f^\nu_{\lambda\mu}(q)$.*

Proof. The idea is to use Green's Formula to initiate an induction. We will see this in the next lecture, so for now we will just state it for the category mod R (so we use that the Euler form vanishes identically). For fixed μ,ν,ξ,η we have

$$\sum_\epsilon F^\epsilon_{\mu\nu}F^\epsilon_{\xi\eta}/a_\epsilon = \sum_{\alpha,\beta,\gamma,\delta} F^\mu_{\alpha\beta}F^\nu_{\gamma\delta}F^\xi_{\alpha,\gamma}F^\eta_{\beta\delta}\frac{a_\alpha a_\beta a_\gamma a_\delta}{a_\mu a_\nu a_\xi a_\delta}.$$

Now suppose we wish to compute $F^\theta_{\mu\nu}$. If S_θ is decomposable, say $\theta=\xi\cup\eta$, then any other extension S_ϵ of S_η by S_ν must satisfy $\theta<\epsilon\leq\xi+\eta$, and so we can write

$$F^\theta_{\mu\nu}F^\theta_{\xi\eta}/a_\theta = \sum_\epsilon F^\epsilon_{\mu\nu}F^\epsilon_{\xi\eta}/a_\epsilon - \sum_{\epsilon>\theta} F^\epsilon_{\mu\nu}F^\epsilon_{\xi\eta}/a_\epsilon.$$

We can apply Green's formula to the first sum on the right and hence express it in terms of Hall numbers involving partitions of size strictly smaller that $|\theta|$, so by induction each of these Hall numbers is given by a universal integer polynomial. Similarly we can apply induction on the dominance order for partitions of size $|\theta|$ to deduce that the Hall numbers appearing in the second sum are also given by universal integer polynomials. Using that the polynomials a_λ are all monic, we conclude that the whole of the right hand side is of the form (integer polynomial)/(monic integer polynomial). Finally, by Riedtmann's Formula, and using that every extension of S_η by S_ξ with middle term S_θ is necessarily split, we see that $F^\theta_{\xi\eta}/a_\theta$ is a quotient of two monic integer polynomials. It therefore follows that $F^\theta_{\mu\nu}$ is of the form (integer polynomial)/(monic integer polynomial), so is itself an integer polynomial by the previous lemma.

It remains to prove the case when S_θ is indecomposable. In this case we saw in §2.1 (3) that the Hall numbers are either zero or one, depending only on the partitions, so we are done. □

6. Macdonald's ring of symmetric functions

Consider the power series ring $\tilde\Gamma := \mathbb{Q}[[X_1,X_2,X_3,\dots]]$. We can describe its elements as follows. Given $\alpha\in\mathbb{N}_0^{(\mathbb{N})}$, set $X^\alpha:=\prod_i X_i^{\alpha_i}$, a finite monomial. Then the elements of $\tilde\Gamma$ are of the form $\sum_\alpha c_\alpha X^\alpha$ with $c_\alpha\in\mathbb{Q}$. We say that a monomial X^α has degree $|\alpha|=\sum_i\alpha_i$, and an element $f\in\tilde\Gamma$ has degree d provided it is of the form $f=\sum_{|\alpha|=d}c_\alpha X^\alpha$. Writing Γ_d for the subspace of elements of degree d, we see that $\Gamma:=\bigoplus_d\Gamma_d$ is a subring of $\tilde\Gamma$.

Now, by regarding X_i as the i-th co-ordinate function on sequences in $\mathbb{Q}^{(\mathbb{N})}$, so $X_i(\underline{x})=x_i$, we can view Γ as a ring of functions $\mathbb{Q}^{(\mathbb{N})}\to\mathbb{Q}$. Then $f\in\Gamma$ has degree d if and only if $f(\lambda\underline{x})=\lambda^d f(\underline{x})$ for all $\lambda\in\mathbb{Q}$ and all $\underline{x}\in\mathbb{Q}^{(\mathbb{N})}$.

Let π be any finitary permutation of $\mathbb{N}$, so π fixes almost all elements. We can then define both $\pi(f)$ for a function f, by setting $\pi(X_i)=X_{\pi(i)}$, and $\pi(\underline{x})$ for a sequence $\underline{x}$, by setting $\pi(\underline{x})_i:=x_{\pi^{-1}(i)}$. It follows that $(\pi(f))(\underline{x})=f(\pi^{-1}(\underline{x}))$. We call a function symmetric provided $\pi(f)=f$ for all finitary permutations π.

Note that the degrees of f and $\pi(f)$ are the same, so π acts on each Γ_n. We write Λ_d for the symmetric functions of degree d, and $\Lambda:=\bigoplus_d\Lambda_d$. This is Macdonald's ring of symmetric functions.

Let us write $\alpha\sim\beta$ provided there exists a finitary permutation π with $\alpha=\beta(\pi)$. Then for each α there exists a unique partition λ with $\alpha\sim\lambda$. Set

$$m_\lambda:=\sum_{\alpha\sim\lambda}X^\alpha.$$

Then the m_λ form a basis for Λ, called the basis of monomial functions. In particular, each graded piece Λ_d is finite dimensional. We also have the following special functions in Λ.

Elementary symmetric functions:

$$e_d := \sum_{|\alpha|=d} X^\alpha, \quad \alpha \in \{0,1\}^{(\mathbb{N})}.$$

Complete symmetric functions:

$$h_d := \sum_{|\alpha|=d} X^\alpha, \quad \alpha \in \mathbb{N}_0^{(\mathbb{N})}.$$

Power sum functions:

$$p_d := \sum_i X_i^d.$$

Each of these forms a set of algebraically-independent generators for Λ. We therefore write, for a partition λ,

$$e_\lambda := \prod_i e_{\lambda_i}, \quad h_\lambda := \prod_i h_{\lambda_i}, \quad p_\lambda := \prod_i p_{\lambda_i},$$

so that each of the e_λ, h_λ and p_λ determines a basis of Λ.

We can relate Λ to the usual rings of symmetric polynomials as follows. For all $m \leq n$ we have compatible embeddings $\mathbb{Q}^m \hookrightarrow \mathbb{Q}^n \hookrightarrow \mathbb{Q}^{(\mathbb{N})}$, given by extending by zero. The polynomial algebra $R_m := \mathbb{Q}[X_1, \dots, X_m]$ can be regarded as polynomial functions on $\mathbb{Q}^m$, and so by restricting functions we obtain compatible surjective algebra homomorphisms $\Gamma \twoheadrightarrow R_n \twoheadrightarrow R_m$. Moreover, these respect the action of finitary permutations, and so we have compatible surjective algebra homomorphisms $\Lambda \twoheadrightarrow S_n \twoheadrightarrow S_m$, where $S_m := R_m^{\mathfrak{S}_m}$ is the usual ring of symmetric polynomials.

In this way we see that, in the category of graded rings

$$\Gamma = \varprojlim R_n \quad \text{and} \quad \Lambda = \varprojlim S_n.$$

Next consider the bijection

$$\mathbb{Q}^{(\mathbb{N})} \times \mathbb{Q}^{(\mathbb{N})} \to \mathbb{Q}^{(\mathbb{N})}, \quad (\underline{x}, \underline{y}) \mapsto \underline{x} \cup \underline{y} := (x_1, y_1, x_2, y_2, \dots).$$

This yields a comultiplication on Λ where

$$\Delta(f) = \sum f' \otimes f'' \quad \text{provided} \quad f(\underline{x} \cup \underline{y}) = \sum f'(\underline{x}) f''(\underline{y}).$$

For, fixing $\underline{y}$, the function $\underline{x} \mapsto f(\underline{x} \cup \underline{y})$ is again in Λ, so can be written as $\sum_\lambda c_\lambda(\underline{y}) m_\lambda$. Moreover, if f has degree d, then we only need to consider partitions λ of size at most d, so this is a finite sum. Now each function $f_\lambda(\underline{y}) = c_\lambda(y)$ is also symmetric, and so we have written $\Delta(f) = \sum_\lambda m_\lambda \otimes f_\lambda$.

From this definition the following identities are clear.

(1) $\Delta(e_d) = \sum_{a+b=d} e_a \otimes e_b$, where $e_0 := 1$.
(2) $\Delta(h_d) = \sum_{a+b=d} h_a \otimes h_b$, where $h_0 := 1$.
(3) $\Delta(p_d) = p_d \otimes 1 + 1 \otimes p_d$.

In this way Λ becomes a commutative and cocommutative Hopf algebra, where the antipode sends p_n to $-p_n$.

6.1. **Extension of scalars.** We now extend scalars and consider the Hopf algebra $\Lambda_t := \Lambda \otimes_{\mathbb{Q}} \mathbb{Q}[t]$. We endow this with a symmetric bilinear form

$$\{p_\lambda, p_\mu\} := \delta_{\lambda\mu} z_\lambda(t),$$

where $z_\lambda(t)$ was defined earlier. This is then a Hopf pairing, which follows by noting that

$$z_{\lambda\cup\mu}(t) = z_\lambda(t) z_\mu(t) \prod_r \binom{a_r + b_r}{a_r}, \quad \lambda = (1^{a_1} 2^{a_2} \cdots), \quad \mu = (1^{b_1} 2^{b_2} \cdots).$$

Thus Λ_t is a self-dual Hopf algebra with this pairing. In fact, this also holds after specialising t to any number which is not a root of unity.

Theorem 6.1. *There is a homomorphism of self-dual Hopf algebras*

$$\Phi\colon \Lambda_t \to H, \quad p_n \mapsto p_n, \quad t \mapsto q^{-1}.$$

The map Φ is an isomorphism if we take the generic Hall algebra (using the Hall polynomials), or just surjective if we take any particular prime power q.

Using generating functions, we show that

$$e_d \mapsto q^{\binom{m}{2}} u_{(1^m)} \quad \text{and} \quad h_d \mapsto \sum_{|\lambda|=m} u_\lambda.$$

6.2. **Hall-Littlewood functions.** The Hall-Littlewood functions $P_\lambda(t)$ are characterised by the two properties:

(1) there exist integer polynomials $b_{\lambda\mu}(t)$ such that

$$P_\lambda(t) = e_{\lambda'} + \sum_{\mu<\lambda} \beta_{\lambda\mu}(t) e_{\mu'}.$$

(2) setting $b_\lambda(t) = \prod_r (1-t)(1-t^2)\cdots(1-t^{m_r})$ for $\lambda = (1^{m_1}2^{m_2}\cdots)$ we have

$$\{P_\lambda(t), P_\mu(t)\} = \delta_{\lambda\mu}/b_\lambda(t).$$

Note that, using the notation introduced earlier, $a_\lambda(t) = t^{d_{\lambda,\lambda}} b_\lambda(t^{-1})$.

The Hall-Littlewood functions have the property that $P_\lambda(0) = s_\lambda$, the Schur function, and $P_\lambda(1) = m_\lambda$, the monomial function. The dual Schur functions $S_\lambda(t)$ are given by taking the dual basis with respect to the symmetric bilinear form. Note that $S_\lambda(0) = s_\lambda$. The Littlewood-Richardson coefficients $c^\nu_{\lambda\mu}$ are the structure constants with respect to the Schur functions, so

$$s_\lambda s_\mu = \sum_\nu c^\nu_{\lambda\mu} s_\nu.$$

It follows that if

$$P_\lambda(t) P_\mu(t) = \sum_\nu g^\nu_{\lambda\mu}(t) P_\nu(t),$$

then the polynomial $g^\nu_{\lambda\mu}(t)$ has constant term $c^\nu_{\lambda\mu}$.

Proposition 6.2. *Under the map $\Phi\colon \Lambda_t \to H$ we have*

$$P_\lambda(t) \mapsto q^{n(\lambda)} u_\lambda, \quad s_\lambda \mapsto b_\lambda, \quad S_\lambda(t) \mapsto b^*_\lambda,$$

where b_λ is Lusztig's canonical basis.

Proof. We just prove the formula for $P_\lambda(t)$. Suppose $|\lambda'| = d$, and write $\lambda' = (a_1, a_2, \ldots)$. Then $(1^{a_1}) \cup (1^{a_2}) \cup \cdots = (1^d)$ and $(1^{a_1}) + (1^{a_2}) + \cdots = \lambda$. Thus

$$e_{\lambda'} \mapsto \sum_{(1^d)\leq\mu\leq\lambda} a_{\lambda\mu}(q) u_\mu,$$

for some polynomials $a_{\lambda\mu}(t)$. Moreover, $a_{\lambda\lambda}(q)$ is non-zero. In fact, the Hall number $F^\lambda_{(1^{a_1})(2^{a_2})\cdots} = 1$ since the corresponding filtration of S_λ has to be the socle filtration, which is unique. Thus $a_{\lambda\lambda}(q) = \sum_i \binom{a_i}{2} = n(\lambda)$, and so

$$P_\lambda(t) \mapsto q^{n(\lambda)} u_\lambda + \sum_{\mu<\lambda} \bar{a}_{\lambda\mu}(q) u_\mu.$$

On the other hand we know that

$$\{u_\lambda, u_\mu\} = \delta_{\lambda\mu} q^{|\lambda|}/a_\lambda(q), \quad \text{so that} \quad \{q^{n(\lambda)} u_\lambda, q^{n(\mu)} u_\mu\} = \delta_{\lambda\mu}/b_\lambda(q).$$

The result follows. ∎

In Macdonald's book he also introduces the functions $q_n(t) = (1-t)P_{(n)}(t)$, which we shall denote by c_n. The c_λ then form the basis dual to the basis of monomial functions, and under Φ the c_n map to the $c_n := (1-q^{-1})u_{(n)}$ discussed earlier.

Comparing the structure constants of the $P_\lambda(t)$ and the u_λ we have

$$f^\nu_{\lambda\mu}(t) = q^{n(\nu)-n(\lambda)-n(\mu)} g^\nu_{\lambda\mu}(t^{-1}).$$

Thus $g^\nu_{\lambda\mu}$ has degree at most $N := n(\nu) - n(\lambda) - n(\mu)$, and

$$f^\nu_{\lambda\mu}(t) = c^\nu_{\lambda\mu} t^N + \text{lower order terms}.$$

In fact, we have the following stronger result.

Theorem 6.3. *The Hall polynomial $f^\nu_{\lambda\mu}$ is non-zero if and only if $c^\nu_{\lambda\mu}$ is non-zero.*

There is no known characterisation of when the Littlewood-Richardson coefficients are non-zero, and although there are various algorithms to compute them explicitly, it is also known that computing them is a P-complete problem.

Proposition 6.4. *The Littlewood-Richardson coefficients satisfy the identity*

$$\sum_\epsilon c^\epsilon_{\lambda\mu} c^\epsilon_{\xi\eta} = \sum_{\alpha,\beta,\gamma,\delta} c^\lambda_{\alpha\beta} c^\mu_{\beta\delta} c^\xi_{\alpha\gamma} c^\eta_{\beta\delta}.$$

Proof. Note that by Riedtmann's Formula, the rational function

$$f^\epsilon_{\xi\eta}(t) t^{d_{\xi,\eta}} a_\xi(t) a_\eta(t)/a_\epsilon(t)$$

counts, for a given DVR R with finite residue field $k = \mathbb{F}_q$, the size of the set $\mathrm{Ext}^1(S_\xi, S_\eta)_{S_\epsilon}$, and so is an integer polynomial. Thus if we take Green's Formula and multiply through by $a_\lambda(q)a_\mu(q)a_\xi(q)a_\eta(q)$, then every term is a Laurent polynomial of degree at most $N = |\lambda| + |\mu| + n(\lambda) + n(\mu) + n(\xi) + n(\eta)$. The identity above is then given by comparing the coefficients of t^N on both sides. □