Iwahori-Hecke-Algebras and James' conjecture
18.10.2007

1 The algebras

Let $n \in \mathbb{N}$, $W :=$ sym. group on $\{1, 2, \ldots, n\}$, $s_i := (i, i+1)$, $S := \{s_1, s_2, \ldots, s_{n-1}\}$.

$$\Longrightarrow W = \langle s_1, \ldots, s_{n-1} \rangle = \langle s_1, \ldots, s_{n-1} \quad | \quad \begin{array}{l} s_i^2 = \mathrm{id}, s_i s_j = s_j s_i \text{ for } |i-j| \geq 2, \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \text{ for } 1 \leq i < n \rangle \end{array}$$

Call $w = t_1 \cdots t_k$ with $t_i \in S$ "reduced expression" if shortest possible.
Def.: Let A com. ring, $v \in A$ invertible.
$\mathcal{H}_n(A, v) :=$ assoc. A-alg. with generators $\{T_s \mid s \in S\}$ subject to relations:

$$\begin{array}{lll} (T_s - v)(T_s + v^{-1}) = 0 & \text{for } s \in S & [v = v \cdot \mathbf{1} \in \mathcal{H}_n(A, v)] \\ T_s T_t = T_t T_s & \text{for } s, t \in S \text{ and } st = ts \text{ and } s \neq t & \\ T_s T_t T_s = T_t T_s T_t & \text{for } s, t \in S \text{ and } st \neq ts. & \end{array}$$

This is called the "Iwahori-Hecke algebra of type A_{n-1} over A with parameter v".
Remark: For $v = 1$: $\mathcal{H}_n(A, 1) = AW$ the group algebra.
Theorem (Bourbaki): For $w \in W$, the element $T_w := T_{t_1} \cdot T_{t_2} \cdots T_{t_k}$ for any reduced expression $w = t_1 \cdots t_k$ with $t_i \in S$ is well-defined and $\{T_w \mid w \in W\}$ is an A-basis of $\mathcal{H}_n(A, v)$.
Corollary: If $\varphi : A \to A'$ is a homomorphism of com. rings, then there is a ring homomorphism

$$\begin{array}{ccccl} \hat{\varphi} & : & \mathcal{H}_n(A, v) & \to & \mathcal{H}_n(A', \varphi(v)) \\ & & T_w & \mapsto & T_w \qquad \forall w \in W \\ & & a & \mapsto & \varphi(a) \qquad \forall a \in A \subseteq \mathcal{H}_n(A, v) \end{array}$$

This is called a "specialisation", because:
If $A = \mathbb{Z}[x, x^{-1}]$, then $\mathcal{H}_n(\mathbb{Z}[x, x^{-1}], x)$ is called the "generic Iwahori-Hecke-Algebra of type A_{n-1}".
Possible specialisations:

$$\begin{array}{ll} \mathcal{H}_n(\mathbb{Z}[x, x^{-1}], x) \to \mathcal{H}(\mathbb{Q}(x), x) & \text{using } \mathbb{Z}[x, x^{-1}] \subseteq \mathbb{Q}(x) \\ \mathcal{H}_n(\mathbb{Z}[x, x^{-1}], x) \to \mathcal{H}(\mathbb{Q}(\zeta_e), \zeta_e) & \text{using } \mathbb{Z}[x, x^{-1}] \to \mathbb{Q}(\zeta_e), x \mapsto \zeta_e \in \sqrt[e]{1} \subseteq \mathbb{C} \\ \mathcal{H}_n(\mathbb{Z}[x, x^{-1}], x) \to \mathcal{H}(\mathbb{F}_p, u) & \text{using } \mathbb{Z}[x, x^{-1}] \to \mathbb{F}_p, x \mapsto u, z \mapsto z + p\mathbb{Z} \end{array}$$

2 Representations and modules

Let A be a field, $\mathcal{H} := \mathcal{H}_n(A, v)$.
Def.: M finite dim. A-vector space. A **representation** of $\mathcal{H}$ is a homomorphism $\varphi : \mathcal{H} \to \mathrm{End}_A(M)$ of A-algebras where $\mathrm{End}_A(M) = \{\alpha : M \to M \mid \alpha \text{ is } A\text{-linear}\}$.
(M, φ) is called an $\mathcal{H}$**-module**. Instead of $\varphi(h)(m)$ for $h \in \mathcal{H}$ and $m \in M$ write $hm = h \cdot m$,
i.e.: $h(m + m') = hm + hm'$ and $(h \cdot h')m = h \cdot (h'm)$ for all $h, h' \in \mathcal{H}$ and $m, m' \in M$.
["Representation theory" studies and classifies the modules of an algebra (up to isomorphism)]

Ex.: Let M_1 be a 1-dim. v.s. over A, then $T_s \mapsto v$ (note $\mathrm{End}_A(M_1) \cong A$) is a representation.
Let M_{-1} be a 1-dim. v.s. over A, then $T_s \mapsto -v^{-1}$ is another one.
Def.: M an $\mathcal{H}$-module. A **submodule** is a sub vector space $N \leq M$, such that $hn \in N \; \forall h \in \mathcal{H} \; \forall n \in N$.
[$\mathcal{H}$-invariant space]
M is called **irreducible**, if it has only the submodules 0 and M.
If $N \leq M$ is a submodule, then M/N is an $\mathcal{H}$-module.
A **composition series** of M is a chain

$$0 = N_0 < N_1 < \cdots < N_r = M$$

of submodules of M, such that N_i/N_{i-1} is irreducible $\forall 1 \leq i \leq r$.
["Representation theory" begins by classifying the irreducible modules.]

Def.: A **partition** λ of n is a tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{N}^k$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$ and $\sum_{i=1}^k \lambda_i = n$. Write $\lambda \vdash n$.
Theorem (Richard Dipper, Gordon James 1986)
Define combinatorically for $\lambda \vdash n$ a "Specht-module" S_v^λ for $\mathcal{H} = \mathcal{H}_n(A, v)$, equipped with a bilinear form $\beta_v^\lambda : S_v^\lambda \times S_v^\lambda \to A$ such that $\beta_v^\lambda(x, y) = \beta_v^\lambda(hx, hy)$ for all $h \in \mathcal{H}$ and all $x, y \in S_v^\lambda$.
Set $\mathrm{rad}(\beta_v^\lambda) := \{x \in S_v^\lambda \mid \beta_v^\lambda(x, y) = 0 \; \forall y \in S_v^\lambda\} \leq S_v^\lambda$. Set $D_v^\lambda := S_v^\lambda / \mathrm{rad}(\beta_v^\lambda)$.

Let $e := e(v)$ be the least number such that $1 + v + v^2 + \cdots + v^{e-1} = 0$ (or $e := \infty$ if none exists).
[this is the multiplicative order of v]
Then:
If $e > n$, then $\mathrm{rad}(\beta_v^\lambda) = 0$ and $D_v^\lambda = S_v^\lambda$ is irreducible. [easy, semisimple case, dimensions known]
If $e \leq n$, then D_v^λ is either irreducible or 0.
Up to isomorphism, $\{D_v^\lambda \mid \lambda \vdash n, D_v^\lambda \neq 0\}$ are all simple modules. [$\lambda = (n)$ and $\lambda = (1^n)$]

3 The conjecture

[Everything solved??? NO!]
Major open problem: For $A = \mathbb{F}_p$, determine $\dim_A(D_v^\lambda)$ for $e \leq n$.

Equivalent: Determine
$[S_v^\lambda : D_v^\mu] :=$ # of occurrences of D_v^μ as factor in a composition series $0 = N_0 < N_1 < \cdots < N_r = S_v^\lambda$, (i.e. $|\{i \mid N_i/N_{i-1} \cong D_v^\mu\}|$, called "**decomposition numbers**").
Remark: E.g. for $A = \mathbb{F}_p$, $p \leq n$, $v = 1 \Longrightarrow e = p$ since $1^0 + 1^1 + 1^2 + \cdots + 1^{p-1} = 0$.
$\to$ modular (i.e. char$A = p$) representations of the sym. group.

Conjecture (James, 1990) Consider $v \in \mathbb{F}_p$, $e := e(v)$ such that $e \cdot p > n$. Then for $\lambda, \nu \vdash n$:

$$\underbrace{[S_v^\lambda : D_v^\mu]}_{\text{for } \mathcal{H}_n(\mathbb{F}_p, v)} = \underbrace{[S_{\zeta_e}^\lambda : D_{\zeta_e}^\mu]}_{\text{for } \mathcal{H}_n(\mathbb{Q}(\zeta_e), \zeta_e)} \qquad \text{(these are known by a deep theorem by Ariki)}$$

with $\zeta_e \in \sqrt[e]{1}\mathbb{C}$ primitive, i.e. decomposition numbers **depend on** $e(v)$ but **not on** p **and** v!
[$\to$ proved in some cases]
E.g.: $\exists$ limit N such that it holds for all $p > N$. **But no explicit limit known!**

4 An equivalent statement

Def.: A field, $(Z, +)$ a totally ordered abelian group. Then $\nu : A \to Z \cup \{\infty\}$ is called a **valuation**, if the following hold:

$$\nu(a) = \infty \iff a = 0$$
$$\nu(a \cdot b) = \nu(a) + \nu(b) \ \forall a, b \in A$$
$$\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$$

Remark: It follows, that $R := \{a \in A \mid \nu(a) \geq 0\}$ is a subring of A with unique maximal ideal $J := \{a \in A \mid \nu(a) > 0\}$, since $\nu(1) = 0$ and thus $\nu(a^{-1}) = -\nu(a)$.
R is a **valuation ring** in A, which means: $\forall 0 \neq a \in A$ we have: a or a^{-1} or both lie in R.
Ex.: Let $A := \mathbb{Q}$, p a prime. Define for $a \in \mathbb{Z} \setminus \{0\}$: $\nu(a) := k$ if $p^k \mid a$ but $p^{k+1} \nmid a$. For $a/b \in \mathbb{Q}$ set $\nu(a/b) := \nu(a) - \nu(b)$.
This gives a valuation on $\mathbb{Q}$ with values in $\mathbb{Z} \cup \{\infty\}$.

Valuation ring $R = \{a/b \mid \gcd(a, b) = 1 \text{ and } p \nmid b\}$
max. ideal $J = \{ap/b \mid \gcd(a, b) = 1 \text{ and } p \nmid b\}$
factor ring $R/J \cong \mathbb{F}_p$

Def.: Call an idempotent $f^2 = f$ **primitive** iff it cannot be written $f = f_1 + f_2$ with two orthogonal idempotents $f_1^2 = f_1$ and $f_2^2 = f_2$ and $f_1 f_2 = 0 = f_2 f_1$.
Assume the situation of James' conjecture: $v \in \mathbb{F}_p$, $e = e(v)$, $e \cdot p > n$ and $\lambda, \mu \vdash n$.
I have defined two valuations
$\nu_1 : \mathbb{Q}(x) \to \mathbb{Z} \cup \{\infty\}$ and $\nu_2 : \mathbb{Q}(x) \to (\mathbb{Z} \times \mathbb{Z}) \cup \{\infty\}$
with valuation rings
$R_i = \{f \in \mathbb{Q}(x) \mid \nu_i(f) \geq 0\}$ and maximal ideals $J_i := \{f \in \mathbb{Q}(x) \mid \nu_i(f) > 0\}$
such that $R_1/J_1 \cong \mathbb{Q}(\zeta_e)$ and $R_2/J_2 \cong \mathbb{F}_p$.
Then: $R_2 \subseteq R_1 \subseteq \mathbb{Q}(x)$ and thus $\mathcal{H}_n(R_2, x)$ embeds into $\mathcal{H}_n(R_1, x)$.
Theorem (N, 2003)
James' conjecture holds if and only iff every primitive idempotent of $\mathcal{H}_n(R_2, x)$ is primitive as idempotent of $\mathcal{H}_n(R_1, x)$.