A Glimpse of Representation Theory

Semra Öztürk

Orta Doğu Teknik Üniversitesi

TKMD 2016 - ATILIM ÜNİVERSİTESİ

Outline

* We assume groups are finite, modules are of finite length, rings are unital and Artinian throughout for simplicity.

– groups, rings, modules, algebras

– simple (irreducible), indecomposable modules, Schur's Lemma;

– semisimple rings, represention theory of group algebras, Maschke's theorem

– simples and indecomposables for cyclic groups, generalized eigenvectors, Jordan c.f.

– modules for noncyclic abelian p-groups in characteristic p

– modules of constant Jordan type, restricted modules that I defined

– conjectures by Suslin, and Rickard for modules of constant Jordan type

– conjectures by Suslin, and Rickard are true for restricted modules that I defined

– only odd or only even size Jordan blocks, Benson's and my theorems

– my conjecture in the case of only odd or only even size Jordan blocks

Groups, Rings, Modules, Algebras

Let X be a set, a bijection $f : X \longrightarrow X$ is a a one to one and onto, hence invertible function.

Let $Sym(X) = \{$ bijections of $X\}$.

Then $(Sym(X), \circ)$ is a group with the composition operation $\circ$ and

the identity element id_X, $id_X(x) = x$ for all x in X.

This is a very natural way of producing groups.

If $X = \{1, 2, \ldots, n\}$, then $Sym(X) = S_n$ has $n!$ elements,

$Sym(X)$ is not commutative for $n \geq 3$, as $f \circ g \neq g \circ f$.

Some group examples are: $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_p^*, .)$

Groups, Rings, Modules, Algebras

Let $(G, *)$ and $(H, \triangle)$ be groups, a function $\alpha : G \longrightarrow H$ is a group homomorphism if $\alpha(x * y) = \alpha(x)\triangle\alpha(y)$ for all x, y in G.

Is the set $Hom(G, H)$ of all group homomorphisms from G to H a group?

Yes, whenever H is commutative! (commutative also referred as abelian)

Let G be any group, $(A, +)$ be an abelian group $\Longrightarrow$ $(Hom(G, A), +)$ is

an abelian group with $(\alpha + \beta)(x) = \alpha(x) + \beta(x)$ for x in G.

If $G = A$, then there is also composition operation $\circ$ in $Hom(A, A)$. Hence $(Hom(A, A), +, \circ)$ is a ring. $Hom(A, A)$ is denoted by $End(A)$ and referred as the endomorphism ring.

This is a very natural way of producing rings.

Some ring examples are : $(\mathbb{Z}, +.\cdot)$, $(\mathbb{Z}_n, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$, $(Mat(n)+, \cdot)$

Groups, Rings, Modules, Algebras

Let R be a ring, let $(M, +)$ be an abelian group M is called a (left) R-module if there is a ring homomorphism $R \to Hom(M, M)$

that is for r, s in R , m, n in $r, s : M \longrightarrow M$ is a group homomorphism for M and $(rs)m = r(sm)$, $1_R m = m$.

Every abelian group is a $\mathbb{Z}$-module; any ring R is an R-module; if $R = F$ is a field, an R-module M is called a vector space.

If M and N are R-modules , then $Hom(M, N) = \{\alpha : M \longrightarrow N \mid \alpha(x + y) = \alpha(x) + \alpha(y)\}$ is also R-module with $r \cdot \alpha \in Hom(M, N)$ defined as $(r \cdot \alpha)(x) = r\alpha(x)$ for x in M.

If R is a commutative ring, then the set of R-module homomorphisms $Hom_R(M, N) = \{\alpha \in Hom(M, N) \mid \alpha(rx) = r\alpha(x)$ for all $r \in R\}$ is also an R-module.

Groups, Rings, Modules, Algebras

A ring R is an algebra over a field F if there is a ring homomorphism $\alpha : F \longrightarrow A$ with $\alpha(F) \subseteq Z(R)$.

Alternatively, a vector space A a field F (of dimension d) is called an algebra (of dimension d) if there is a bilinear multiplication on A.

Some examples are:

– polynomial ring $F[x]$,

– $End_F(M) = Hom_F(M, M)$ where M is a vector space over F,

– the ring of $n \times n$ matrices over F,

– group algebras $F[G]$ where G is a group.

$F[G]$ is a vector space with basis G, and group multiplication induces a multiplication with $(cg)(dh) = (cd)(gh)$ for c, d in F, g, h in G.

Subgroups, Subrings, Submodules

A subset K which is closed under the operations of the set S is a subobject, for instance S is a group, or ring, or R-module.

A map $f : S \longrightarrow T$ between two sets S, T having the same structure is called a homomorphism if it preserves the structure.

Special subojects are kernels of homomorphisms:

Let $f : S \longrightarrow T$ be a homomorphism ;

if S and T are groups, then $\ker(f) = \{s \in S \mid f(s) = id_T\}$,

if S and T are rings, or R-modules, then $\ker(f) = \{s \in S \mid f(s) = 0_T\}$.

If S is a group, or a ring, or an R-module, then $S/\ker(f)$ is of the same structure as S.

Simplicity

Let S be a group , or a ring S is called simple if any homomorphism $f : S \longrightarrow T$ is a monomorphism or $|f(S)| = 1$.

An R-module M is called simple (or irreducible) if it has no submodules other than 0 and M itself.

$(\mathbb{Z}_p, +)$ is a simple group and also simple as a $\mathbb{Z}$-module.

$(\mathbb{Z}_p, +, \cdot)$ is a simple ring.

If M is R-module $\Longrightarrow$ Rm is a submodule for $m \in M$.

If M is simple $m \neq 0 \Longrightarrow Rm = M$ and the map $R \longrightarrow M = Rm$ given by $r \mapsto rm$

has kernel denoted by $Ann_R(m)$, so that $R/Ann_R(m) \cong Rm$.

Schur's Lemma

If M and N are simple R-modules, then every R-module homomorphism between M and N is the zero homomorphism or an isomorphism,

i.e., $\left(\text{Hom}_R(M, N) \neq 0 \iff M, N \text{ are isomorphic.}\right)$

In particular, if $M = N$, then $End_R(M) := Hom_R(M, M)$ is a division ring as well; (division ring is a ring such that every non-zero element has inverse)

Consequences:

1) If F is algebraically closed, and R is an F-algebra, M is a simple R-module, then $End_R(M) \cong F$,
(that is, every R-homomorphism is multiplication by an element of F.)

2) If R is a commutative algebra over an algebraically closed field F, and M is a simple R-module, then $dim_F(M) = 1$.

Proof of 1) and 2)

Proof 1). Let $T \in Hom_R(M, M)$, then T is a linear map. Since F is algebraically closed, T has an eigenvalue $\lambda \in F$. Then $T - \lambda id_M \in Hom_R(M, M)$. Since there is corresponding eigenvector $m \neq 0$ in M, $(T - \lambda id_M)(m) = 0$. So $T - \lambda id_M$ is not an isomorphism. By Schur's Lemma $T - \lambda id_M = 0$, that is $T = \lambda id_M$.

Proof 2). Since R is commutative then for any $r \in R$, $\theta_r : M \longrightarrow M$, given by $\theta_r(m) = rm$ is an R-module homomorphism as $\theta_r(sm) = rsm = srm$ for any $s \in R$. By (1) $\theta_r = \lambda id_M$ for some $\lambda \in F$. Let N be a 1-dimensional subspace of M, and $r \in R$. Since $\theta_r = \lambda id_M$, $rn = \lambda n \in N$, hence N is R-module. Simce M is simple $M = N$ is 1-dimensional.

Counter-example for 1) If $F = R$ reals and $M = \mathbb{C} = R \oplus Ri$, $\phi : \mathbb{C} \longrightarrow \mathbb{C}$ $\phi(z) = iz$ is R-linear, and $\phi^2 = -id_{\mathbb{C}}$ but there is no $r \in R$ with $\phi = r \cdot id_{\mathbb{C}}$ because $r^2 \neq -1$ for all $r \in R$.

Direct Sums, Indecomposability for modules

Let S and T have the same algebraic structure, both are groups, or both rings, both are R-modules, $\Longrightarrow$ their direct sum $S \oplus T = \{(s,t) \mid s \in S,\ t \in T\}$ has the same structure with coordinatewise operations.

Let M be R-module , **M is called indecomposable if whenever $M \cong N \oplus K$ with submodules K, N we have N or K is 0.**

Simplicity and indecomposability is determined also by the structure of the ring $End_R(M)$:

M is simple $\Longleftrightarrow$ f is isomorphism or $f = 0$ for all $f \in End_R(M)$.

M is indecomposable $\Longleftrightarrow$ f is isomorphism or $f^k = 0$ for some $k \geq 1$ (f is nilpotent) for all $f \in End_R(M)$.

Examples:

$\mathbb{Z}_n$ is a $\mathbb{Z}$-module for any n, when $n = p$ is a prime **$\mathbb{Z}_p$ is simple**

$\mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ for primes $p \neq q$ but $\mathbb{Z}_p \oplus \mathbb{Z}_p \ncong \mathbb{Z}_{p^2}$

$\mathbb{Z}_p$ is a subgroup of $\mathbb{Z}_{p^2}$ so **$\mathbb{Z}_{p^2}$ is not simple but indecomposable**

$K \oplus H \ncong \mathbb{Z}_{p^2}$ for any H, K.

Indecomposability and Projections

Let M be an R-module, $f \in Hom_R(M, M)$ is called a projection if $f^2 = f$.

If f is a projection, then $id_M - f$ is also a projection;
$(id_M - f)^2 = id_M - 2f + f^2 = id_M - f$.

A projection gives a direct sum decomposition with submodules of M because;

$id_M = f + id_M - f$, and $f(id_M - f) = f - f^2 = 0$ implies

$M = image(f) \oplus \ker(f)$.

In fact; if $f_1, \ldots, f_k \in Hom_R(M, M)$ with $f_i^2 = f$, and $f_i f_j = 0$ for $i \neq j$,

$id_M = f_1 + \cdots + f_k$ and $M \cong f_1(M) \oplus \cdots \oplus f_k(M)$.

Examples : 1) The zero map $f = 0$ and $f = id_M$ are trivial projections

2) Let $M = \mathbb{R} \oplus \mathbb{R}$ be the $\mathbb{R}$-vector space of dimension 2, and $f(a, b) = (a, 0)$, then

$f(f(a, b)) = f(a, 0) = (a, 0) \Longrightarrow f^2 = f$.

Semisimple rings

A ring R is called semisimple if every R-module M can be written as $M \cong M_1 \oplus \cdots \oplus M_k$ where M_i is simple R-modules.

Example: Any field $F = R$ is semisimple, every vectorspace $M \cong F^k$ for some k.

Non-example : $R = \mathbb{Z}$ is not semisimple $\mathbb{Z}_{p^2}$ is indecomposable but not isomorphic to direct sum of simples.

So, if there are indecomposable R-modules $\Longrightarrow$ R is not semisimple

R is not semisimple $\Longrightarrow M \cong M_1 \oplus \cdots \oplus M_k$ where M_i is indecomposable

Observation: Let $0 \neq v \in M$, $0 \neq Rm$ is a submodule of M .

M simple $\Longrightarrow M = Rm$ and $R/Ann_R(m) \cong Rm$ as R-modules, and $Ann_R(m)$ is a maximal left ideal

R is not semisimple if $J(R) \neq 0$ where $J(R) = \cap\{Ann_R(M) : M \ simple\}$.

R = F, M is a vector space

M simple F-module $\Longrightarrow M \cong F$

$M \cong F^m$ and $N \cong F^n$ then $Hom_F(M,N) \leftrightarrow Mat_{n\times m}(F)$

$f \in Hom_F(M,N), \Longleftrightarrow f(cv) = cf(v)$ and $f(v+w) = f(v) + f(w)$

$f : M \longrightarrow N$

M has a basis, say , $v_1, \ldots, v_m$, every element of M is of the form $c_1 v_1 + \cdots + c + m v_m$

N has a basis, say , $u_1, \ldots, u_n$, every element of N is of the form $d_1 u_1 + \cdots + d_n u_n$

so knowing f means knowing $f(v_i) = d_{i1} u_1 + \cdots + d_{in} u_n$, $i = 1, \ldots, m$

so $f \leftrightarrow (d_{ij}) = \left(\quad d_{ij} \quad \right)$

Representation Theory

$\{abstract\ algebraic\ structures(groups, associativealgebras, posets)\} \Longrightarrow$

$\{concrete\ objects\ in\ linear\ algebra,\ matrices\}$

Example :

$\{finite\ groups\} \Longrightarrow \{associate\ group\ elements\ with\ matrices\}$

Let G be group, a representation of G of dimension n over F is a group homomorphism

$\theta : G \longrightarrow GL_n(F)$ so that

$\theta(g)$ is matrix A and $A^{order(g)} = I$.

Representation Theory of Finite Groups

The group homomorphism

$\theta : G \longrightarrow GL_n(F^n)$ can be extended linearly to a ring homorphism

$\Theta : F[G] \longrightarrow End_F(F^n) \cong Mat_{n\times n}(F)$

Hence F^n is an $F[G]$-module via Θ.

Representation theory of $F[G]$ becomes $F[G]$-module theory.

Depending on the characteric of the field, $F[G]$ is semisimple or non-semisimple.

These two cases are totally different.

For instance, if G is abelian, non-cyclic p-group, all indecomposable (simple) $\mathbb{C}G$-modules are known, but if characteristic of F is p, classification for indecomposables exists only for $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Theorems on the number of simples, indecomposables

– If A is a finite dimensional F-algebra, and F is algebraically closed, then there are finitely many simple A-modules up to isomorphism. If their degrees are d_i, then $\Sigma_i d_i^2 = dim_F(A) - dim_F J(A)$ where $J(A)$ is the largest nilpotent left ideal in A.

– If $A = F[G]$ where G is a p-group and $char(F) = p$, then $dim_F(A) - dim_F J(A) = 1$, so that there is only one irreducible module which is 1-dimensional.

–(Higman) Let F be a field of characteristic p. There are finitely many indecomposable $F[G]$-modules if and only if a Sylow subgroup of G is cyclic .

– If G is cyclic p-group of order p^n, F is a field of characteristic p, then there p^n non-isomorphic indecomposable $F[G]$-modules.

– (Schur) If G is abelian and F is algebraically closed, M simple $F[G]$-module, then $dim_F(M) = 1$ and $Hom)R(M, M) \cong F$.

Observation

Note that $(\Sigma_{g\in G} g)h = h(\Sigma_{g\in G} g) = \Sigma_{g\in G} g$ for any $h \in G$

then $(\Sigma_{g\in G} g)F[G] = (\Sigma_{g\in G} g)F \cong F$ is a submodule of $F[G]$ fixed by G and

$(\Sigma_{g\in G} g)(\Sigma_{g\in G} g) = \mid G \mid (\Sigma_{g\in G} g)$.

If $\mid G \mid$ has an inverse in F, then $r_G = \frac{1}{|G|}\Sigma_{g\in G} g$ is a projection in $F[G]$ because;

$r_G^2 = (\frac{1}{|G|}\Sigma_{g\in G} g)(\frac{1}{|G|}\Sigma_{g\in G} g) = (\frac{1}{|G|})^2(\Sigma_{g\in G} g)(\Sigma_{g\in G} g) = (\frac{1}{|G|})^2 \mid G \mid (\Sigma_{g\in G} g) = r_G$.

In particular, $F[G] \cong r_G F[G] \oplus (1 - r_G)F[G]$ so that $F[G]$ is not indecomposable.

If $\mid G \mid = 0$ in F, then $(\Sigma_{g\in G} g)$ is a nilpotent element in $F[G]$, then $F[G]$ is not semisimple.

$\mid G \mid$ has an inverse in $F \iff char(F)$ does not divide $|G|$

Maschke's Theorem

Maschke's Theorem Suppose $char(F)$ does not divide $|G|$ and M be anf $F[G]$-module. If N is a submodule of M, then there is a submodule W such that $M = N \oplus W$.

Proof: Note that M is a vector space over F and F is semisimple, so there is a subspace V of M such that $M = N \oplus V$. We want to obtain a submodule though. Let $pr_V : M \longrightarrow V$ be the projection onto V, $pr_V(n, v) = v$. Using pr_V define an $F[G]$-homomorphism $f : M \longrightarrow M$ by $f(m) = \frac{1}{|G|}\Sigma_{g\in G} g^{-1} pr_V(gm)$. This f is a projection as well, $f^2 = f$, and $f(M) = V$, so that $M = V \oplus \ker(f)$.

By this theorem every $F[G]$-module is a direct sum of irreducibles, that is, $F[G]$ is semisimple.

If $char(F) = 0 \Longrightarrow F[G]$ is semisimple.

$\mathbb{R}[G]$, $\mathbb{C}[G]$ are semisimple.

Restricting M to a subgroup H, $\mathbf{M\downarrow_H}$

Chouinard's Theorem and Dade's Lemma, modular case

Let M be an $F[G]$-module and $H \leq Units(F[G])$ be a subgroup.

Then $F[H]$ is a subalgebra of $F[G]$, and M is an $F[H]$-module denoted by $M\downarrow_H$.

An elementary abelian p-group E of order p^n is of the form $E = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (n-copies).

Chouinard's Theorem* (1976) Let G be a finite p-group, an $F[G]$-module M is free if and only if $M\downarrow_E$ is free for every elementary abelian p-subgroup E of G.

*To avoid some definitions we state Chouinard's theorem in a special case.

Dade's Lemma (1978) An $F[E]$-module M is free if and only if $M\downarrow_{\langle 1+x \rangle}$ is free for all x in $J(E) \backslash J(E)^2$.

PART 2

Examples of Representations of Cyclic Group

Let $G = \langle g \rangle \cong \mathbb{Z}_k$, and F be any field. An $F[G]$-module/representation of dimension n is given by a homomorphism $\phi : G \longrightarrow GL_n(F) = Aut(F^n)$.

ϕ is determined by a matrix $A = \phi(g)$ with $A^k = I_n$, that is, $M = F^n$

$g : M \longrightarrow M$ is linear and $[g]_{\mathcal{B}} = A$ where $\mathcal{B}$ is a basis for G.

– $M = F$ is trivial $F[G]$-module, $A = [c]$ with $c^k = 1$ (F must have k-th root of 1.)

– $M = F[G]$ is the regular $F[G]$-module.

– $M = I$ is a left ideal of $F[G]$, is an $F[G]$-module.

$\mathbb{C}\mathbb{Z}_5$, semisimple case, char$(\mathbb{C}) = 0 \neq 5$

Suppose $F = \mathbb{C}$, $G = \langle g \rangle \cong \mathbb{Z}_5$ and M is a simple $\mathbb{C}[G]$-module.

By Schur's Lemma $dim_{\mathbb{C}}(M) = 1$ and $[g] = [\omega]$, where $\omega^5 = 1$, so $gm = \omega m$ for all $m \in M$.

There are 5 possibilities for ω, so there are five simple $\mathbb{C}G$-modules all of dimension 1.

Problem: Write the regular module $\mathbb{C}[G]$ as a sum of simple modules. Let $A = [g]_B$ where $\mathcal{B} = \{1, g, \ldots, g^{k-1}\}$ is a basis for $\mathbb{C}[G]$. Then $A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$ and the characteristic polynomial of A is
$\det(xI - A) = x^5 - 1 = (x - \omega_1)(x - \omega_2)(x - \omega_3)(x - \omega_4)(x - 1)$ where $\omega_i^5 = 1$.

There are 5 distinct roots, so A is diagonalizable. A is similar to
$D = \begin{bmatrix} \omega_1 & 0 & 0 & 0 & 0 \\ 0 & \omega_2 & 0 & 0 & 0 \\ 0 & 0 & \omega_3 & 0 & 0 \\ 0 & 0 & 0 & \omega_4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ therefore

$\mathbb{C}\mathbb{Z}_5 = M_1 \oplus \cdots \oplus M_5$, such that M_i is simple and $rm_i = \omega_i m_i$ for $m_i \in M_i$.

$F\mathbb{Z}_5$, modular case, char$(F) = 5$

Let $G = \langle g \rangle \cong \mathbb{Z}_5$. Let M be a simple $F[G]$-module. Assume F is algebraically closed.

By Schur's Lemma $dim_F(M) = 1$ and $[g] = [\omega]$, with $\omega^5 = 1$. Since F is a field, $0 = \omega^5 - 1 = (\omega - 1)^5 \mod (5)$ implies $\omega = 1 \mod (5)$.
Therefore $M = F$ and $gm = m$ for all $m \in M$.
So there is only one simple $F[G]$-module, $M = F$, it has trivial g-action.

Problem: Write the regular module FG as a sum of indecomposable modules.

$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$. The characteristic polynomial of

$A = \det(xI - A) = x^5 - 1 = (x-1)^5$, then 1 is the only eigenvalue, it has multiplicity 5. However, since $rank(A - I) = rank(R) = 4$, the eigenspace of 1 is 1-dimensional, so that A is not diagonalizable;

$$A - I = \begin{bmatrix} -1 & 0 & 0 & 0 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix} \sim \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix} = R .$$

Generalized Eigenvectors

Definition: A vector v_m is called a generalized eigenvector of rank m of a matrix A corresponding to the eigenvalue λ, if

$$(A - \lambda I)^m v_m = 0, \qquad (A - \lambda I)^{m-1} v_m \neq 0.$$

The set $\{v_m, (A-\lambda I)v_m, (A-\lambda I)^2 v_m, (A-\lambda I)^3 v_m, \ldots, (A-\lambda I)^{m-1} v_m\}$ is linearly independent and

$v_1 = (A - \lambda I)^{m-1} v_m$, then $(A - \lambda I)v_1 = 0$, so $Av_1 = \lambda v_1$

$v_2 = (A - \lambda I)^{m-2} v_m$, then $v_1 = (A - \lambda I)v_2$, so $Av_2 = v_1 + \lambda v_2$

$\vdots$

$v_{m-1} = (A - \lambda I)v_m$, then $\quad Av_m = v_{m-1} + \lambda v_m$.

The Jordan block of A corresponding to the eigenvalue λ written with respect to this basis is the form

$$\begin{bmatrix} \lambda & 0 & 0 & 0 & 0 \\ 1 & \lambda & 0 & 0 & 0 \\ 0 & 1 & \lambda & 0 & 0 \\ 0 & 0 & 1 & \lambda & 0 \\ 0 & 0 & 0 & 1 & \lambda \end{bmatrix}$$

For $F\mathbb{Z}_5$

Let $N = A - I$, let's compute powers of N:

$$N = \begin{bmatrix} -1 & 0 & 0 & 0 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix}, \; N^2 = \begin{bmatrix} 1 & 0 & 0 & 1 & -2 \\ -2 & 1 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 & 0 \\ 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 1 & -2 & 1 \end{bmatrix},$$

$$N^3 = \begin{bmatrix} -1 & 0 & 1 & -3 & 3 \\ 3 & -1 & 0 & 1 & -3 \\ -3 & 3 & -1 & 0 & 1 \\ 1 & -3 & 3 & -1 & 0 \\ 0 & 1 & -3 & 3 & -1 \end{bmatrix}, \; N^4 = \begin{bmatrix} 1 & 1 & -4 & 6 & -4 \\ -4 & 1 & 1 & -4 & 6 \\ 6 & -4 & 1 & 1 & -4 \\ -4 & 6 & -4 & 1 & 1 \\ 1 & -4 & 6 & -4 & 1 \end{bmatrix},$$

$$N^5 = \begin{bmatrix} 0 & -5 & 10 & -10 & 5 \\ 5 & 0 & -5 & 10 & -10 \\ -10 & 5 & 0 & -5 & 10 \\ 10 & -10 & 5 & 0 & -5 \\ -5 & 10 & -10 & 5 & 0 \end{bmatrix}, \; N^6 = \begin{bmatrix} -5 & 15 & -20 & 15 & -5 \\ -5 & -5 & 15 & -20 & 15 \\ 15 & -5 & -5 & 15 & -20 \\ -20 & 15 & -5 & -5 & 15 \\ 15 & -20 & 15 & -5 & -5 \end{bmatrix},$$

$F\mathbb{Z}_5$, modular case $\mathrm{char}(F) = 5$

In our example above, $(A-I)^5 = A^5 - I^5 = I - I = 0$, but do not know $(A-I)^4 \neq 0$.

$-1 = 4 \mod (5)$, $-2 = 3 \mod (5)$, etc.

$$A - I = \begin{bmatrix} 4 & 0 & 0 & 0 & 1 \\ 1 & 4 & 0 & 0 & 0 \\ 0 & 1 & 4 & 0 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 1 & 4 \end{bmatrix}, \ (A-I)^2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 3 \\ 3 & 1 & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 3 & 1 \end{bmatrix},$$

$$(A-I)^3 = \begin{bmatrix} 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 2 & 3 & 4 \end{bmatrix}, \ (A-I)^4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \neq 0,$$

$$(A-I)^5 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = 0, \ (A-I)^6 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = 0,$$

$F\mathbb{Z}_5$, modular case , char$(F) = 5$

In our example above, $(A-I)^5 = A^5 - I^5 = I - I = 0$, and $(A-I)^4 \neq 0$.

Since $(A-I)^4 \neq 0$, there is a non-zero vector v_5 with $(A-I)^4 v_5 \neq 0$. Let

$v_1 = (A-I)^4 v_5$,
$v_2 = (A-I)^3 v_5$,
$v_3 = (A-I)^2 v_5$,
$v_4 = (A-I) v_5$.

Then $(A-I)v_1 = 0$, so that $Av_1 = v_1$, v_1 is an eigenvector and v_2, v_3, v_4, v_5 are generalized eigenvectors for A corresponding to 1.

The set $\mathcal{B} = \{v_5, v_4, v_3, v_2, v_1\}$ is linearly independent and
$v_4 = (A-I)v_5 = Av_5 - v_5$ so that $Av_5 = v_4 + v_5$
$v_3 = (A-I)^2 v_5 = (A-I)v_4 = Av_4 - v_4$ so that $Av_4 = v_3 + v_4$
$v_2 = (A-I)^3 v_5 = (A-I)v_3 = Av_3 - v_3$ so that $Av_3 = v_2 + v_3$
$v_1 = (A-I)^4 v_5 = (A-I)v_2 = Av_2 - v_2$ so that $Av_2 = v_1 + v_2$

Rewriting the matrix A using the basis $\mathcal{B}$ we obtain the Jordan form J of A,

$$J = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \sim A.$$ Therefore $F\mathbb{Z}_5$ is indecomposable.

$F\mathbb{Z}_5$, modular case, shifted basis

We obtained the matrix A of the generator g using the basis $\{1, g, g^2, \ldots, g^4\}$ for $F\mathbb{Z}_5$.

If we used the basis $\{1, g-1, (g-1)^2, \ldots, (g-1)^4\}$ for $F\mathbb{Z}_5$, then

$$[g-1] = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \text{ and adding } I \text{ gives } [g] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

which is already in the Jordan form.

A nilpotent matrix with 5th power zero can be the matrix of $[g-1]$ action on an $F\mathbb{Z}_5$-module M.

M is indecomposable $F\mathbb{Z}_5$-module if there is only one Jordan block in the Jordan form of $[g-1]$. All other possible Jordan blocks are

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 \end{bmatrix},$$ which correspond to indecomposable modules V_4, V_3, V_2, V_1 respectively, $dim(V_i) = i$. Vi 's are submodules (ideals of) $F[G]$. Note also that $F[G]$ is indecomposable and contains all the indecomposables.

Modular Case, Indecomposables for a Cyclic p-group,

Let $\mathbf{Z}_{p^t} = \langle g \rangle$. All the indecomposables are submodules (ideals) of $F[G]$.

There is a unique maximal ideal $J(F[G])$ of dimension $p^t - 1$, with $(J(F[G]))^i$ of dimension $p^t - i$.

Using the shifted basis $\{(g-1)^{p^t-1}, (g-1)^{p^t-2}, \ldots, g-1, 1\}$ for $F[G]$ we can write explicitly $(J(F[G]))^i$.

Let $V_i = (J(F[G]))^i = Span\{\, (g-1)^{p^t-1}, \ldots, (g-1)^{p^t-i}\,\}$ for $i = 1, 2, \ldots, p^{t-1}$.

The action of $g-1$ on V_i is represented by the $i \times i$ nilpotent Jordan matrix $[i]$.

$V_1 = k, V_2, \ldots V_{p^t-1}, \ldots V_{p^t} = F[\langle g \rangle]\}$ is the set of all indecomposable $F[\langle g \rangle]$-modules, hence a $F[\langle g \rangle]$-module M of dimension d is of the form

$M \cong V_1^{b_1} \oplus \cdots \oplus V_{p^t}^{b_{p^t}}$ where $\Sigma_{i=1}^{p^t} i b_i = d$.

M is completely determined by $\mathbf{b} = (b_1, \ldots, b_{p^t})$ where b_i-many Jordan blocks $[i]$.

b is called the p^t-Jordan type of M also of $X = [g-1]$.

It is easy to compute b_i, namely, $b_i = X^{i-1} - 2X^i + X^{i+1}$.

Key observation

The decomposition of M in terms of indecomposable $k[\mathbf{Z}_{p^t}]$-modules completely determines the decomposition of the restriction $M\downarrow_{\mathbf{Z}_{p^s}}$ of M for the subgroups $\mathbf{Z}_{p^s} = \langle g^{p^{t-s}} \rangle$ contained in $\mathbf{Z}_{p^t} = \langle g \rangle$ for $s \leq t$.

Hence, if $\underline{b}$ is p^t-Jordan type of M as a $k[\langle g \rangle]$-module and $\underline{a}$ is the p^s-Jordan type of M as a $k[\langle g^{p^{t-s}} \rangle]$-module, then

$$a_i = p^s b_{ip^s} + \Sigma_{j=1}^{p^s-1} j \left[b_{(i-1)p^s+j} + b_{(i+1)p^s-j} \right].$$

In this case, we say $\underline{a}$ **is a p^{t-s}-restricted p^s-Jordan type** and **write $\underline{a}$=$\underline{b}\downarrow_{t-s}$.** The coefficients of b_j's appearing in a_i form a nice pattern. For $p = 5$, $t = 2$, $s = 1$;

$$a_1 = b_1 + 2b_2 + 3b_3 + 4b_4 + 5b_5 + 4b_6 + 3b_7 + 2b_8 + b_9,$$

$$a_2 = b_6 + 2b_7 + 3b_8 + 4b_9 + 5b_{10} + 4b_{11} + 3b_{12} + 2b_{13} + b_{14},$$

$$a_3 = b_{11} + 2b_{12} + 3b_{13} + 4b_{14} + 5b_{15} + 4b_{16} + 3b_{17} + 2b_{18} + b_{19},$$

$$a_4 = b_{16} + 2b_{17} + 3b_{18} + 4b_{19} + 5b_{20} + 4b_{21} + 3b_{22} + 2b_{23} + b_{24},$$

$$a_5 = b_{21} + 2b_{22} + 3b_{23} + 4b_{24} + 5b_{25}.$$

PART 3

Representations of $\mathbb{Z}_{p^t} \times \mathbb{Z}_{p^s}$, modular case

Let $G = \langle g, h : g^{p^t} = 1 = h^{p^s}, gh = hg \rangle \cong \mathbb{Z}_{p^t} \times \mathbb{Z}_{p^s}$, and k be of characteristic p.

Since $\mathbb{Z}_{p^t} \times \mathbb{Z}_{p^s} \geq \mathbb{Z}_p \times \mathbb{Z}_p$, Higman's Theorem implies that there are **infinitely many indecomposable** $k[G]$**-modules**.

There is **no classification** for indecomposable modules over $k[\mathbb{Z}_p \times \mathbb{Z}_p]$ except for $p = 2$.

A $k[G]$-module/representation of dimension d is given by a homomorphism $\phi : G \longrightarrow GL_d(k) = Aut(k^d)$.

ϕ is determined by $\phi(g)$ and $\phi(h)$.

Let $A = \phi(g)$, $B = \phi(h)$.

Then $A^{p^t} = I$, $B^{p^s} = I$ and $AB = BA$.

The characterstic of k is p, then $(A - I)^{p^t} = A^{p^t} - I = I - I = 0$ similarly for B.

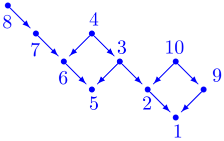
To make computations easier, we work with $X = A - I$, and $Y = B - I$ corresponding to $g - 1$ and $h - 1$ respectively.

Visualizing modules for $\mathbb{Z}_{p^t} \times \mathbb{Z}_{p^s}$, modular case

A way of visualizing an $k[\mathbf{Z}_{p^t} \times \mathbf{Z}_{p^s}]$-module M:

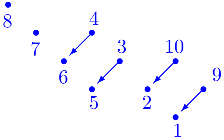
southwest arrow denotes multiplication by $g - 1$,
and southeast arrow denotes multiplication by $h - 1$, g and h are the group generators.

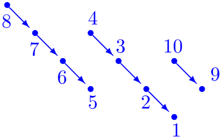
For example let $G \cong \mathbb{Z}_4 \times \mathbb{Z}_4$,



$M \downarrow_{\langle h \rangle}$ has 4-Jordan type $(0, 1, 0, 2)$ (right fig.)

$M \downarrow_{\langle g \rangle}$ has 4-Jordan type $(2, 4, 0, 0)$ (left fig.)





Constant Jordan Type Modules

Let E be an elementary abelian group of order p^r with generators $e_1, \ldots e_r$.

Let $\alpha = (\alpha_1, \ldots, \alpha_r) \in k^r$ not all $\alpha_i = 0$, define $x_\alpha = \alpha_1(e_1 - 1) + \ldots + \alpha_r(e_r - 1)$.

In characteristic p,

$x_\alpha^p = \alpha_1^p(e_1 - 1)^p + \ldots + \alpha_r^p(e_r - 1)^p = 0$ because $(e_i - 1)^p = e_i^p - 1 = 1 - 1 = 0$.

$x_\alpha \in J(k[E])$, $\qquad \mathbb{Z}_p \cong \langle 1 + x_\alpha \rangle \leq Units(k[E])$.

An $k[E]$-module is said to be of **constant Jordan type** if $M \downarrow_{\langle 1+x_\alpha \rangle}$ has the same decomposition for all α in $k^r \backslash 0$.

That is, the Jordan canonical form of the matrix of x_α is the same for all α in $k^r \backslash \mathbf{0}$.

These modules are introduced by Carlson-Friedlander-Pevtsova in 2008

Let A be an abelian p-group, that is, $A \cong \mathbb{Z}_{p^{t_1}} \times \ldots \times \mathbb{Z}_{p^{t_m}}$.

I generalized the above definition to constant p^t-Jordan type for $k[A]$-modules in 2011.

A $k[A]$-module is said to be **of constant p^t-Jordan type** if the p^t-Jordan type of M is the same for all subgroups $\mathbf{Z}_{p^t}$ of the **unit group of** $k[A]$ for which $k[A]$ is a free $k[\mathbf{Z}_{p^t}]$-module.

Two examples of constant Jordan type modules $\mathbf{Z}_5 \times \mathbf{Z}_5$

The $k[\mathbf{Z}_5 \times \mathbf{Z}_5]$-modules M and M', given in Figure 5 and Figure 6 respectively, both are constant Jordan type modules.

The Jordan types of M and M' are

$(1, 1, 3, 0, 0)$ and $(1, 2, 1, 1, 0)$, respectively.

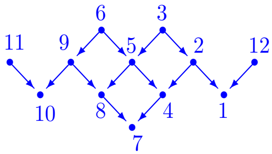


Figure 5.

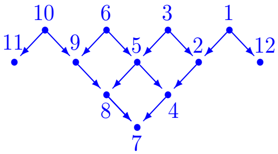


Figure 6.

Conjectures by Suslin and Rickard on Jordan types

There are more conjectures than results on Jordan types of $k[E]$-modules of constant Jordan type as it is a difficult problem even for $E = \mathbf{Z}_3 \times \mathbf{Z}_3$.

Suslin's Conjecture. *If M is a $k[\mathbf{Z}_p \times \mathbf{Z}_p]$-module of constant Jordan type having no Jordan blocks of sizes $i-1$, and $i+1$, then there is no Jordan block of size i, for $2 < i < p$, and $p > 3$.*

Rickard's Conjecture. *If M is a $k[E]$-module of constant Jordan type having no Jordan block of size i then the total number of Jordan blocks of size at least i is divisible by p.*

Benson verified Rickard's conjecture for the special case $i = 1$.

Key observation

The decomposition of M in terms of indecomposable $k[\mathbf{Z}_{p^t}]$-modules completely determines the decomposition of the restriction $M{\downarrow}_{\mathbf{Z}_{p^s}}$ of M.

For instance , $\mathbb{Z}_5 \cong \langle g^5 \rangle \;\leq\; \langle g \rangle \cong \mathbb{Z}_{25}$,

if $\underline{b}$ is 5^2-Jordan type of M as a $k[\langle g \rangle]$-module and

$\underline{a}$ is the 5-Jordan type of $M\downarrow_{\langle g^5 \rangle}$.

$$a_i = 5b_{i5} + \Sigma_{j=1}^{4} j\left[b_{(i-1)5+j} + b_{(i+1)5-j}\right].$$

Recall that the coefficients of b_j's appearing in a_i form a nice pattern. ;

$$a_1 = b_1 + 2b_2 + 3b_3 + 4b_4 + 5b_5 + 4b_6 + 3b_7 + 2b_8 + b_9,$$

$$a_2 = b_6 + 2b_7 + 3b_8 + 4b_9 + 5b_{10} + 4b_{11} + 3b_{12} + 2b_{13} + b_{14},$$

$$a_3 = b_{11} + 2b_{12} + 3b_{13} + 4b_{14} + 5b_{15} + 4b_{16} + 3b_{17} + 2b_{18} + b_{19},$$

$$a_4 = b_{16} + 2b_{17} + 3b_{18} + 4b_{19} + 5b_{20} + 4b_{21} + 3b_{22} + 2b_{23} + b_{24},$$

$$a_5 = b_{21} + 2b_{22} + 3b_{23} + 4b_{24} + 5b_{25}.$$

My conjecture generalizing Suslin and Rickard's

Conjecture B. Suppose that M is a $k[A]$-module of constant p^t-Jordan type $\underline{a}$.

If $a_i = a_l = 0$, then p^s divides the sum $\Sigma_{j=i}^{l} a_j$, for $1 \leq i < l \leq p^t$.

When $A = E$, this is Rickard's Conjecture and Modified Suslin's Conjecture.

Conjecture B is **true for restricted** $k[A]$-modules by my Theorem A (2014).

Theorem A. *Suppose that A is an abelian p-group, M is a p^s-restricted $k[A]$-module, and $\underline{a}$ is the p^t-Jordan type of M at a p^s-restricted p^t-point x of A with $p > 3$. If $a_i = a_l = 0$, then p^s divides the sum $\Sigma_{j=i}^{l} a_j$, for $1 \leq i < l \leq p^t$.*

Restricted Modules

If G is an abelian p-group of order divisible by p^t and A is a proper subgroup of index at most p^{t-s} for $s \leq t$, then $\langle g^{p^{t-s}} \rangle \cong \mathbf{Z}_{p^s}$ is a subgroup of A for $g \in G$ of order p^t.

Hence there will be p^{t-s}-restricted p^s-Jordan types. This motivated the definition of restricted modules.

A $k[A]$-module M is called a p^{t-s}**-restricted module** if there is such a G and a $k[G]$-module N isomorphic to M as a $k[A]$-module.

So, a $k[A]$-module M is a p^{t-s}**-restricted module** of constant if M is restricted module and it is of constant Jordan type.

Example of a restricted module for $\mathbf{Z}_2 \times \mathbf{Z}_4$

Figure 5 represents a 10-dimensional $k[\mathbf{Z}_2 \times \mathbf{Z}_4]$-module. Its restriction to $\mathbf{Z}_2 \times \mathbf{Z}_2$ is a restricted $k[\mathbf{Z}_2 \times \mathbf{Z}_2]$ module is a **direct sum the modules in Figure 2 and Figure 3.**

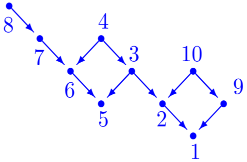


Figure 5.

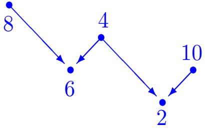


Figure 2.

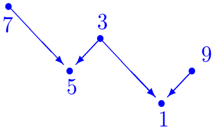


Figure 3.

Only odd/only even Jordan blocks case by Benson

Theorem (Benson, 2010). There cannot be a $k[E]$-module of constant Jordan type $\underline{a}$=$(0, a_2, \ldots, a_{p-2}, 0, *)$ where $a_i = 0$ for all $i \in \{2, \ldots, p-2\}$ except for one i for which $a_i = 1$.

Theorem (Benson, 2011) Suppose that a $k[E]$-module M has constant Jordan type with only distinct odd sizes or l only of distinct even sizes. Then the Jordan type of M is of the form $\underline{a}$=$(1, 0, \ldots, 0, *)$ or $\underline{a}$=$(0, \ldots, 0, 1, *)$, or $\Sigma_{i=1}^{p} a_i \geq 4$.

Theorem (Benson, 2013) Suppose that a $k[E]$-module M has constant Jordan type $(a_1, \ldots, a_t, 0, \ldots, 0, *)$ with $\Sigma_i^t a_i \leq min(r-1, p-2)$, then Jordan type of M is of the form $\underline{a}$=$(1, 1, 1, 1, a_t = 1, 0, \ldots, 0, *)$ where r is the E is of rank r.

Corollary. Suppose that a $k[E]$-module M has constant Jordan type and E is of rank r, $p > r$, with Jordan type $(a_1, 1, 0 \ldots, 0, *)$, then then $a_1 \geq r - 2$.

My only odd/only even Jordan bloks results and a conjecture implied by it

Theorem C. Suppose that M is a restricted $k[A]$-module of constant p^t-Jordan type having only odd size or of only even size.
Then the Jordan type of M is of the form

$(p^s t_1 + r, 0, p^s t_3, 0, p^s t_5, 0, \ldots, 0, p^s t_{p^t})$ for some integer $r \geq 0$ or
$(0, p^s t_2, 0, p^s t_4, 0, \ldots, 0, a, *)$ for integers t_i, a, $* \geq 0$ with $p^s \mid a + *$.

Theorem D. Suppose that M is a restricted $k[A]$-module of constant p^t-Jordan type.
Then Jordan type is of the form $(a, b, 0, \ldots)$, then $a \geq p - b$.
In particular, if $p - 1 \geq r - s$, then $a \geq r - s$ for $s \geq r$;
if $b \neq 0$, then $a \neq 0$.

By **removing the hypothesis "restricted"** from our theorems we can state many conjectures, such an example is in the next page.

A conjecture

Conjecture E. Suppose that M is a $k[A]$-module of constant p^t-Jordan type with only odd size or of only even sizes.
Then the Jordan type of M is of the form

$(p^s t_1 + r, 0, p^s t_3, 0, p^s t_5, 0, \ldots, 0, p^s t_{p^t})$ for some integer $r \geq 0$ or
$(0, p^s t_2, 0, p^s t_4, 0, \ldots, 0, a, *)$ for integers t_i, a, $* \geq 0$ with $p^s \mid a + *$.

Conjecture E is true for restricted $k[A]$-modules of constant p^t-Jordan type.

References

D. Benson, *Modules of constant Jordan and a conjecture of Rickard*, J. Algebra, 393, **2014** , 343-349

D. Benson , Modules of Constant Jordan Type with Small Non-Projective Part, Algebr. Represent. Theory, 16, **2013** , no. 1, 29–33.

D. Benson, *Modules of constant Jordan type with one non-projective block* Algebr. Represent. Theory 13,**2010**, 315-318.

S.Öztürk Kaptanoğlu, *Restricted modules and conjectures for modules of constant Jordan type*, Algebr. Represent. Theor , 17, **2014** , 14371455.

S.Öztürk Kaptanoğlu, *p-power points and modules of constant p-power Jordan type*, Communications in Algebra, 39, **2011**, 3781-3800.

J. F. Carlson, E. Friedlander, A. Suslin, *Modules for* $\mathbf{Z}/p \times \mathbf{Z}/p$, Comment. Math. Helv., 86, **2011**, 609–657.

J. F. Carlson, E. Friedlander, J. Pevtsova, *Modules of constant Jordan type*, J. Reine Angew. Math. 614, **2008**, 191–234.