Representation Theory and Practice

Richard Parker

Spring 2010

Personal background.

- The group theorists of the 1960's, 1970's and 1980's are now either dead, retired or at least very old.
- In this company I am a young man.
- I studied under J. H. Conway on the "*Atlas"* project and learned lots of tricks.
- I wish to pass some of this on before it is too late!

Why study representation theory?

First part – probably about 10 lectures.

- How ordinary representation theory can be used to study a finite group.

Remainder – probably about 14 lectures.

- Modular representations are interesting in their own right, although modular representation theory can also be used to prove things about groups.

Any comments?

- What would you like me to cover.
- I will ask for answers at the end of this lecture.

Why is representation theory so powerful?

- The product of two conjugacy classes in a group is the sum of conjugacy classes.
- So $C_i \times C_j = \Sigma\, a_{ijk} C_k$
- Knowing the integers a_{ijk} is ***equivalent*** to knowing (the character of) all the representations over the complex numbers.

Finite group as matrices over an arbitrary field.

- Over the complex numbers it is a very pretty theory – ordinary representations.
- Arbitrary fields of characteristic zero and characteristic coprime to group order are "similar" to ordinary representations.
- If the characteristic divides the group order, theorems are weaker so it is harder to get info about the representations

We could let G be a finite group and F be an arbitrary field. . .

- Can make initial definitions
- Can prove many of the critical theorems.
- We could get further with this approach. Tensor products and induced representations always work irrespective of the field.
- But the proofs are often easier if you do not try to work in the widest generality.
- So I decided not to be strict about this.

DO NOT CONFUSE Decomposable / Reducible

- **Decomposable** means representation is the direct sum.

  * 0

  0 *
- **Reducible** means it has an invariant subspace, but not necessarily a complementary space.

  * *

  0 *

Study of indecomposables

- If we want to know all the representations of G over F ***up to isomorphism.***
- Hard- verging on the impossible.
- What are the representations mod 2 of 2x2x2? "Wild".

Study of irreducibles

- Only finitely many for each group.
- Relatively easy.
- I do not expect to find out the degrees of the monster's irreducibles mod 2 in my lifetime.
- But most other problems seem tractable.
- If all else fails we can make the matrices on a computer if they are not too big.

S3 mod 2 is **Decomposable**

- Action of S3 (permutations on three points) has invariant subspace over any field – indeed fixed vector – [1 1 1].
- Mod 2 we can find a complementary space of vectors whose sum is 0 namely space spanned by [1 1 0] and [1 0 1]
- So representation is the direct sum of two smaller representations and that defines it up to isomorphism.

S3 mod 3 is **Reducible** but not **Decomposable**

- [1 1 1] is still invariant and indeed fixed.
- But vectors whose sum is zero, namely [1 2 0] and [1 0 2] is no longer a complementary space, since it includes the fixed vector (twice the sum of the above two).
- It is mainly this problem that makes modular (Brauer) representation theory less tidy.

Two important theorems for all fields.

- **Jordan-Hölder.** If we iterate reduction, the **irreducibles** we get as composition factors are well-defined (up to order).
- **Krull-Schmidt.** If we iterate decomposition, the **indecomposables** we get as direct summands are well-defined (up to order). Krull-Schmidt is not that easy to prove.

Jordan-Hölder – sketch of proof

- Suppose we have two maximal chains of invariant subspaces.
- If they start with the same minimal invariant subspace, use induction.
- Otherwise the two minimal invariant subspaces span an invariant subspace W
- In this case we can go via a chain with their direct sum W as an invariant subspace.

Regular representation – only finitely many irreducibles.

- Use basis b_x indexed by group elements x.
- Take R(g) as the (permutation) matrix that takes b_x to $b_{(xg)}$
- Any irreducible representation S is a quotient of that! Pick any non-zero vector v, then map b_x to v.S(x).
- Hence if you "chop up" the regular representation into irreducibles, you must get all of them.

What about indecomposables?

- There are a finite number of indecomposables over a field of characteristic p if and only if the Sylow-p subgroup of G is cyclic (or trivial).
- If the Sylow-p subgroup is not cyclic, you probably do not want to try to classify all indecomposable representations.
- (can be done for C2 x C2)

Maschke's theorem

- If the characteristic is 0 or does not divide the group order, every reducible representation decomposes, so there is no difference between the two concepts.
- The good but easy proof is by making the average over G-images of an arbitrary initial projection onto the subspace.
- This works provided we can divide by the order X of G (and otherwise we are stuck).

Some details of proof of Maschke's theorem.

- If we have an invariant subspace W in a group of order X
- Start with any old projection r from V -> W (so that r(w)=w for w in W)
- Define $r'(v) = \Sigma_g\, r(v.g) / X$ [If we can!]
- But kernel of r' is G-invariant
- Since $r'(v.h) = \Sigma_g\, r(v.g.h) / X$ $= \Sigma_g\, r(v.g) / X = r'(v.h)$ since we have just permuted the terms

Mashke's theorem consequences.

- If it holds, all the main properties of the representations are determined by the "ordinary character table" which is independent of the field.
- Many powerful numerical facts are available.
- The theory is so "clean" that one can readily use it without knowing much about the group!

Example

- Suppose G is any finite group with an element t of order 2 whose centralizer is S = C2 x C2 and that all three elements of order two in S are conjugate in G.
- This information is sufficient to calculate the character table of G (two cases). If character values on t are {1, 1, -1, -1} the character table is determined to be . . .

Example – A5

	60	4	3	5	5
p power		A	A	A	A
p' part		A	A	A	A
ind	1A	2A	3A	5A	5B
+	1	1	1	1	1
+	3	-1	0	-b5	*
+	3	-1	0	*	-b5
+	4	0	1	-1	-1
+	5	1	-1	0	0

The class multiplication table

- The product of two conjugacy classes is the sum of conjugacy classes.
- This gives a commutative associative ring – the centre of the group algebra.
- If Maschke's theorem holds, this algebra is diagonalizable.
- We can therefore tabulate the 1-dimensional components of this ring.

Example – A5

1A	2A	3A	5A	5B	
					2A x 3A
1	15	20	12	12	300 20.6
1	-5	0	4b5	*	0
1	-5	0	*	4b5	0
1	0	5	-5	-5	0
1	3	-4	0	0	-12

Worked example of structure constants.

1A	**2A**	**3A**	**5A**	**5B**	
0	*4*	*6*	*5*	*5*	*2A x 3A*
1	**15**	**20**	**12**	**12**	*300*
1	**-5**	**0**	**4b5**	*	*0*
1	**-5**	**0**	*	**4b5**	*0*
1	**0**	**5**	**-3**	**-3**	*0*
1	**3**	**-4**	**0**	**0**	*-12*

Interests of the Audience

- Proving things about general groups [Studying groups that do not exist]
- Using character tables to prove things about particular groups [Studying groups that do exist].
- Studying representations for their own sake?
- Something else?

Representations – Theory and Practice – Lecture 2

Properties of ordinary character tables

Revision from last time

- Over the complex numbers every representation is the direct sum of irreducibles. There are only a finite number of them for a given group.

I'll go straight to characters.

- Given a complex irreducible representation ρ
- And an element g of G
- The corresponding ***character*** is the trace in ρ of g – denoted by $\chi_\rho(g)$.
- Notice that $M^{-1}.\rho(g).M$ has the same trace as ρ(g) so the character does not depend on which element of the class you take, nor on which basis you use for ρ

Character table tabulates . . .

- Columns indexed by conjugacy classes g.
- Rows indexed by irreducible complex representations ρ
- Entries are traces (in the complex numbers) $\chi_\rho(g)$.
- For A5, note that b5 = [-1+sqrt(5)]/2 and * means negate sqrt(5).

Get ready to concentrate hard!

- Loads of facts about complex representations coming up. Need to learn what is true first, as then can use some facts to prove other facts.
- Also, proof can depend on context
  - Prime characteristic not dividing group order needs careful definition of character and indicator which I'll deal with later.
  - Characteristic zero also get Schur Index questions which I'll also go into a bit later

Properties of character tables

1. Table is square
2. Column orthogonality
3. Row orthogonality
4. Indicator +1, 0 or -1 (+,o,- in *Atlas*)
5. Congruent (mod p) to p-part
6. Structure constant formula
7. Central characters are algebraic integers
8. Degrees divide the group order.
9. Characters characterise representations
10. Formula for number of square roots

1. Table is Square

- There are precisely as many distinct irreducibles as there are conjugacy classes.

2. Column Orthogonality

- $\Sigma_\rho \chi_\rho(g).\chi_\rho(g)^\complement = |\text{Centralizer}(g)|$
- In particular the sum of the squares of the degrees is the order of the group.
- $\Sigma_\rho \chi_\rho(g).\chi_\rho(h)^\complement = 0$ (g not conjugate to h)

A5

	60	4	3	5	5	2A.2A	1A.2A
p power		A	A	A	A		
p' part		A	A	A	A		
ind	1A	2A	3A	5A	5B		
+	1	1	1	1	1	1	1
+	3	-1	0	-b5	*	1	-3
+	3	-1	0	*	-b5	1	-3
+	4	0	1	-1	-1	0	0
+	5	1	-1	0	0	1	5

3. Row Orthogonality

- $1/|G| \; . \; \Sigma_g \chi_\rho(g).\chi_\rho(g)^\complement = 1$
- $[1/|G|] \; . \; \Sigma_g \chi_\rho(g).\chi_\sigma(g)^\complement = 0$ (ρ and σ distinct)

A5

	60	4	3	5	5	
p power		A	A	A	A	
p' part		A	A	A	A	
ind	1A	2A	3A	5A	5B	
+	1	1	1	1	1	
+	3	-1	0	-b5	*	
+	3	-1	0	*	-b5	
+	4	0	1	-1	-1	
+	5	1	-1	0	0	
(4.5)	20	+	20.-1		[/60]	= 0
(5.5)	25 + 15		+ 20		/60	= 1

4. Indicator +1, 0 or -1

- Indicator of $\rho = 1/|G| \cdot \Sigma_g \chi_\rho(g^2) \varepsilon \{1,0,-1\}$
- **Indicator = +1** character is real and ρ is writable over the reals, fixing a quadratic form.
- **Indicator = -1** character is real but ρ is ***not*** writable over the reals, complex representation fixes a symplectic form.
- **Indicator = 0** character is not real (so representation certainly isn't)

A5

	60	4	3	5	5
p power		A	A	A	A
p' part		A	A	A	A
ind	1A	2A	3A	5A	5B
+	1	1	1	1	1
+	3	-1	0	-b5	*
+	3	-1	0	*	-b5
+	4	0	1	-1	-1
+	5	1	-1	0	0

5 +15.5+20.-1+12.0+12.0 / 60 = +1

5. Congruent mod p to p-part

- If an element x has order $p^\alpha.r$ with (p,r)=1, then x has a unique expression as y.z where y and z are powers of x, y has order p^α, z has order r. We say that z is the p' part of x (and y is the p-part).
- Then $\chi_\rho(x) \equiv \chi_\rho(z) \pmod p$
  [i.e. $\chi_\rho(x) - \chi_\rho(z)$ lies in an ideal dividing p]

Example – A5

	60	4	3	5	5	
p power		A	A	A	A	Check that 3A
p' part		A	A	A	A	and 1A are
ind	1A	2A	3A	5A	5B	congruent (mod 3)
+	1	1	1	1	1	
+	3	-1	0	-b5	*	
+	3	-1	0	*	-b5	
+	4	0	1	-1	-1	
+	5	1	-1	0	0	

6. Structure constant formula

- $X(g,h,k) = S(g,h,k) \cdot |G|^2 / C(g,h,k)$
- X(g,h,k) means number of ordered triples conjugate to g,h and k respectively with product 1
- $S(g,h,k) = \Sigma_\rho \chi_\rho(g).\chi_\rho(h).\chi_\rho(k)/\chi_\rho(1)$
- C(g,h,k) means |C(g)|.|C(h)|.|C(k)|

Example – A5

	60	4	3	5	5
p power		A	A	A	A
p' part		A	A	A	A
ind	1A	2A	3A	5A	5B
+	1	1	1	1	1
+	3	-1	0	-b5	*
+	3	-1	0	*	-b5
+	4	0	1	-1	-1
+	5	1	-1	0	0

C(2A,2A,2A)=4.4.4 = 64 X = S . 60^2 / C
X(2A,2A,2A)= (15.2) = 30
S(2A,2A,2A)=1-1/3-1/3+1/5 = 8/15

7. Central characters are algebraic integers.

- Central character is
  Character value . Class size / degree

So called because it is a character of the centre of the group algebra.

Example – A5

1A	2A	3A	5A	5B	Character value x
1	15	20	12	12	Class size ÷
1	-5	0	4b5	*	Degree
1	-5	0	*	4b5	=
1	0	5	-5	-5	Algebraic
1	3	-4	0	0	Integer

8. Degrees divide the group order.

- Actually the degree divides <index of the centre>
- Though that is harder to prove.

9. Characters characterize

- If two representations (irreducible or otherwise) have the same character on every conjugacy class, they are equivalent.
- That is why we call them characters

10. Formula for number of square roots of an element.

- Number of square-roots of g
- = Σ_ρ indicator(ρ) . $\chi_\rho(g)$.

A5

	60	4	3	5	5	
p power		A	A	A	A	
p' part		A	A	A	A	
ind	1A	2A	3A	5A	5B	
+	1	1	1	1	1	
+	3	-1	0	-b5	*	
+	3	-1	0	*	-b5	
+	4	0	1	-1	-1	
+	5	1	-1	0	0	
	16	0	1	1	1	number sqrts.

Row orthogonality I

- A matrix X with $\rho(g)X = X\sigma(g)$ for all g is called a "hom".
- Homs are clearly closed under addition.
- The map $w \rightarrow w.X$ is a homomorphism from the space that ρ acts on into the space that σ acts on.
- $w.X.\sigma(g)=w.\rho(g)X$
- It is an isomorphism between a "sub" of σ and a "quotient" of ρ

Row orthogonality II

- Now take any matrix M
- Since $\rho(gh)^{-1} = \rho(h)^{-1}\rho(g)^{-1}$ we have $M \rightarrow \rho(g)^{-1}M\sigma(g)$ is a representation
- So if we add up all its G-images we get a matrix X invariant under G
- $X = \rho(g)^{-1}X\sigma(g)$ or $\rho(g)X = X\sigma(g)$

Row orthogonality III

- If we take ρ and σ where we know that there are no homs (e.g. distinct irreducibles)
- We get that X must be zero!
- Starting with M=0 except one 1 in the i,j position, and looking at the p,q entry of the resulting matrix X we get that the sum over g of $\rho_{pi}(g^{-1})$and σ_{jq}
- Hence we get that $\Sigma_g \chi_\rho(g^{-1}).\chi_\sigma(g)= 0$

Representations – Theory and Practice – Lectures 3 (and 4)

The hard work of getting started with ordinary character theory!

"Schur's lemma"
Character table is square.
Row Orthogonality
Column Orthogonality
"Frobenius-Schur" indicator

Schur's lemma

- The only matrices that commute with an absolutely irreducible representation are the scalar multiples of the identity.
- This is true for any field.
- It's probably true for some other things that are not fields if you can define "absolutely irreducible".

Commutant

- Suppose we are given a representation as matrices which I denote by ρ(g). To start with, entries are in some ring – not necessarily a field at this stage.
- The ***commutant*** is the set of matrices X that commute with all the ρ(g) – that is to say $X.\rho(g) = \rho(g).X$ for all g in G.
- Call this set of matrices hom(ρ, ρ)

Simple properties of the commutant

- $(X+Y)\rho(g) = \rho(g).(X+Y)$
- $XY.\rho(g) = \rho(g).XY$
- If X is invertible, $X^{-1}.\rho(g) = \rho(g).X^{-1}$
- 0 and 1, and indeed all scalars are in the commutant.
- It is an associative ring.
- Kernel and image of any X is G-invariant.

Now suppose we have a field

- Eigenspaces of a commutant matrix **decompose** the representation.
- Hence if the eigenvalues are not all the same, if we adjoin them to the field we can decompose our representation.
- If our representation is indecomposable, all the eigenvalues must be the same.
- If our representation is irreducible, the non-zero elements of the commutant are invertible, so form a division ring.

Division ring facts

- The centre is a field, and the dimension over the centre is a square.
- The only division rings finite dimensional over the reals are :– the reals, the complex numbers and the quaternions.
- [Wedderburn] All finite division rings are fields – the centre is all of it.
- Over the rationals, there are oodles of them.

Schur's lemma.

- The only matrices that commute with an absolutely irreducible representation are the scalar matrices.
- All the eigenvalues must be the same, and if you subtract that scalar (also in the commutant) the result is singular so zero.

The group ring

- Take a set of indeterminates x_g indexed by the elements of the group
- The group ring is the set of formal sums $\Sigma a_g x_g$ with complex numbers a_g
- Addition is component wise
- Define multiplication by $x_g x_h = x_{gh}$
- This gives an associative ring with identity.
- And an action of G defined by $x_g \rho(h) = x_{gh}$

The centre of the group ring.

- On one hand, it obviously has a basis consisting of the class sums – the sum of x_g for g in a given conjugacy class.
- On the other hand as a representation it can be diagonalized into the irreducibles and the centre is then the scalars on the irreducibles.
- Hence the dimensions of these two must be the same.
- (and shows us why the sum of the squares of the degrees comes to the group order).

Diagonalized regular representation.

A
B
B
B
C
C
C
C

3. Row Orthogonality

- $1/|G| \cdot \Sigma_g \chi_\rho(g).\chi_\rho(g)^\complement = 1$
- $[1/|G|] \cdot \Sigma_g \chi_\rho(g).\chi_\sigma(g)^\complement = 0$ (ρ and σ distinct)

A5

	60	4	3	5	5	
p power		A	A	A	A	
p' part		A	A	A	A	
ind	1A	2A	3A	5A	5B	
+	1	1	1	1	1	
+	3	-1	0	-b5	*	
+	3	-1	0	*	-b5	
+	4	0	1	-1	-1	
+	5	1	-1	0	0	
(4.5)	20	+	20.-1			[/60] = 0
(5.5)	25 + 15		+ 20			/60 = 1

Hom

- For any two representations ρ and σ of the same group over the same field (any field!), a matrix X with $\rho(g).X = X.\sigma(g)$ for all g is called a "hom".
- "Hom" is short for "homomorphism" because any such matrix is a G-invariant homomorphism from the vector space acted on by ρ ***into*** that of σ. We will need homs again later. You can add them.

$\rho(g).X = X.\sigma(g)$

- Let us define W to be the image of X. It is clearly a subspace of σ, and is G-invariant since w in W means there is a v with v.X=w. But $w.\sigma(g) = v.X.\sigma(g) = v.\rho(g).X$ showing that $w.\sigma(g)$ is also in the image of X.
- We may use σ to define an action of G on it, since W is G-invariant. Now X is clearly a homomorphism from ρ onto W.

One can try to make a hom very easily.

- Take any matrix M (right size and shape)
- and take $X = \Sigma_g[\rho(g)^{-1}M\sigma(g)]$
- $\rho(h)^{-1}X\sigma(h)$ is just the same sum in a different order since

  $\rho(h)^{-1}\rho(g)^{-1}M\sigma(g)\sigma(h) = \rho(gh)^{-1}M\sigma(gh)$
- So $X = \rho(h)^{-1}X\sigma(h)$ or $\rho(h)X = X\sigma(h)$
- Hence $X = \Sigma_g[\rho(g)^{-1}M\sigma(g)]$ is a hom.

If there is no non-zero hom – e.g. ρ and σ distinct irreducibles. . .

- Take M to be the matrix with 1 in the i,j position and zero everywhere else.
- M.σ(g) is a matrix that is zero except that row i is the j-row of σ(g).
- $\rho(g)^{-1}M\sigma(g)$ is therefore column i of $\rho(g)^{-1}$ tensored with row j of σ(g).
- Sum this over g and you must get the zero matrix – the only hom there is.

$\Sigma_g \chi_\rho(g).\chi_\sigma(g)^¢=0$

- Let us define $L_{i,j}(\sigma,g)$ to be the i,j entry in σ(g).
- Then we have proved the very strong orthogonality result that
- $\Sigma_g[L_{i,j}(\rho,g^{-1})*L_{k,l}(\sigma,g^{-1})]=0$ for all I,j,k,l
- Note that $\chi(g)^¢=\chi(g^{-1})$ since the eigenvalues are all roots of 1.
- So $\Sigma_g \chi_\rho(g)^¢.\chi_\sigma(g)=$
  $\Sigma_g[\Sigma_i L_{i,i}(\rho,g^{-1})*\Sigma_j L_{j,j}(\sigma,g)]=0.$

$\Sigma_g \chi_\rho(g).\chi_\rho(g)^¢ = |G|$

- By Schur's lemma a hom from ρ to itself is a scalar, so still zero off the diagonal, and entirely zero if the trace of M is zero.
- $\Sigma_g[L_{i,j}(\rho,g^{-1})*L_{k,l}(\rho,g)]=0$ unless i=l so LHS=
- $\Sigma_{g,i}[L_{i,i}(\rho,g^{-1})*L_{i,i}(\rho,g)]$. But for any given i this is the i,i entry of a scalar matrix whose trace is clearly the order of G, being the sum of that many matrices of trace 1. QED

Column orthogonality relations

- We have just shown that if C is the character table and D is the class sizes written down the diagonal, then $C.D.C^†=G$.
  ($C^†$ means transpose complex conjugate)
- Since the character table is square, C/|G| and $D.C^†$ are inverses, whence $D.C^†$. C/|G| is also the identity.
- Hence $C^†C$ is $|G|.D^{-1}$ so is the centralizer orders written down the main diagonal.

4. Indicator +1, 0 or -1

- Indicator of $\rho = 1/|G| . \Sigma_g \chi_\rho(g^2) \varepsilon \{1,0,-1\}$
- **Indicator = +1** character is real and ρ is writable over the reals, fixing a quadratic form.
- **Indicator = -1** character is real but ρ is ***not*** writable over the reals, complex representation fixes a symplectic form.
- **Indicator = 0** character is not real (so representation certainly isn't)

A5

	60	4	3	5	5
p power		A	A	A	A
p' part		A	A	A	A
ind	1A	2A	3A	5A	5B
+	1	1	1	1	1
+	3	-1	0	-b5	*
+	3	-1	0	*	-b5
+	4	0	1	-1	-1
+	5	1	-1	0	0

5 +15.5+20.-1+12.0+12.0 / 60 = +1

Tensor product of ρ and σ

- One way to define $\rho \mathbf{x} \sigma$ is as the set of rectangular matrices M, with the action of G given by (primed means transpose).

  $M.\rho \mathbf{x} \sigma(g) = \rho'(g).M.\sigma(g)$.
- Diagonalizing ρ(g) and σ(g), one can readily see that $\chi_{\rho x \sigma}(g) = \chi_\rho(g) * \chi_\sigma(g)$.

When is there a fixed point in $\rho \mathbf{x} \rho$ for ρ absolutely irreducible?

- $\rho'(g).M.\rho(g)=M$ if ρ is irreducible implies M is non-singular so $M^{-1}.\rho'(g^{-1}).M=\rho(g)$.
- Hence (for any field!) if the dual $\rho'(g^{-1})$ and ρ(g) are not isomorphic we say that the indicator is **O**.
- Transposing $\rho'(g).M.\rho(g)=M$ we get $\rho'(g).M'.\rho(g)=M'$ showing that if M is a fixed point so is M'.

If the dual $\rho'(g^{-1})$ and ρ(g) ***are*** isomorphic.

- M dualizes ρ and M'^{-1} brings it back, so $M.M'^{-1}$commutes so is a scalar. Hence $M'=\lambda M$. Since $M''=M$ we must have $\lambda^2=1$. All such matrices have the same λ so we can take it as a definition of indicator provided the characteristic is not 2.

Indicator in odd characteristic

- If ρ is absolutely irreducible and the dual $\rho'(g^{-1})$ and ρ(g) are isomorphic, there is a matrix M that conjugates ρ(g) to $\rho'(g^{-1})$ such that $M' = \pm M$.
- If $M' = M$ we say that the indicator is **+**
- If $M' = -M$ we say that the indicator is **-**

Representations – Theory and Practice – Lecture 4

More proofs (work)

Characters characterise.
Indicators
Central characters algebraic integers
Degrees divide group order
Structure constant formula
Congruences
Formula for square roots

Characters characterize

- Since (for example) the row orthogonality relations hold . . .
- The rows of the character table are linearly independent.
- But there are only as many ordinary irreducibles as there are conjugacy classes.
- Hence the character must determine the isomorphism type of the representation.

Given a representation with character ψ, find its constituents.

- Let me use the symbol H(c) for the class size of c.
- We merely need to find the inner product $(\psi,\chi)=\Sigma_c H(c)\psi(c).\chi(c)^¢/|G|$ to find out how many copies of each irreducible χ are in ψ.
- In particular, the trivial character appears $\Sigma_c H(c)\psi(c)/|G|$ times, since in that case the character $\chi^¢$ takes the value 1 on every class.

Definition of indicator of an irreducible in any characteristic.

- If the representation is not self-dual, the indicator is **O**.
- If the representation fixes a quadratic form, the indicator is **+**
- If the representation is self-dual but does not fix a quadratic form the indicator is **−**

What is a quadratic form?

- (Getting it right in characteristic 2!)
- A quadratic form is a map Q(v) from the set of vectors to the field and a [necessarily symmetric] bilinear form B(v,w) to the field such that
- Q(v+w)=Q(v)+Q(w)+B(v,w)

In characteristic 2

- Indicators are a bit tricky.
- It is sometimes difficult to determine whether a self-dual representation fixes a quadratic form.
- So difficult, in fact, that in the last resort we use the computer to actually make the fixed form if there is one.
- I will return to characteristic 2 quadratic forms later in the course.

Characteristic zero

- The matrix conjugating a representation ρ to its dual is either symmetric or skew symmetric (not both in odd characteristic!)
- To find out which, we determine the character of the action on each part, then take the inner product with the trivial character.

Symmetric and skew square.

- In any characteristic ρ**x**ρ, given as $M.\rho\mathbf{x}\rho(g) = \rho'(g).M.\rho(g)$ has the symmetric and the skew-symmetric matrices M as invariant subspaces.
- To see this we note that . . .
- If M'=M then $[M.\rho\mathbf{x}\rho(g)]' = [\rho'(g).M.\rho(g)]' = \rho'(g).M'.\rho(g) = \rho'(g).M.\rho(g) = M.\rho\mathbf{x}\rho(g)$.
- Similarly with a minus sign suitably interspersed.

What is the character of the actions?

- If the eigenvalues of $\rho(g)$ are λ_i, the eigenvalues of the action on skew-symmetric matrices are just the products of eigenvalues from distinct pairs $\Sigma\lambda_i\lambda_j$ which is clearly $[(\Sigma\lambda_i)^2 - \Sigma\lambda_i^2]/2$.
- Hence the character is $[\chi^2(g)-\chi(g^2)]/2$
- Similarly the character on the symmetric matrices is $[\chi^2(g)+\chi(g^2)]/2$ since we now include the diagonal.

Over the complex numbers

- Reminder – skew square is $[\chi^2(g)-\chi(g^2)]/2$
- If the representation is self-dual we know that the tensor square contains 1. Hence $\Sigma_g\chi^2(g)$ is $|G|$
- Therefore the indicator is **+** if and only if $\Sigma_g[\chi(g^2)] = |G|$.
- and the indicator is **−** if and only if $\Sigma_g[\chi(g^2)] = -|G|$.

If the indicator of a complex representation is **+**

- Its character values are all real
- It can be written over the real numbers.
- That real representation fixes a positive definite quadratic form.

If the indicator of a complex representation of degree d is **−**

- Its character values are all real.
- It cannot be written over the real numbers dimension d
- It can be written over the complex numbers in dimension d, and that representation fixes a symplectic form.
- There is a real representation of degree 2.d, and the matrices that commute with that are isomorphic to the quaternions.

If the indicator of a complex representation is **0**.

- There is a non-real character value
- So it certainly cannot be written over the reals.
- It is not isomorphic to its dual
- Like all complex representations it can still be written as a unitary representation.

Central characters are algebraic integers.

- The central characters are the eigenvalues of the matrix corresponding to multiplication of the centre of the group algebra by a single class sum.
- This matrix consists of ordinary integers.
- Hence the eigenvalues are algebraic integers.
- $[H(c)\chi(c)/\deg]$.

Degrees divide the group order

- Inner product of character with itself gives $\Sigma_c \; H(c)\chi(c) \; . \; \chi(c)^{¢} = |G|$
- But $H(c)\chi(c)/deg$ is a central character so an algebraic integer.
- So is $\chi(c)^{¢}$ - sum of roots of unity.
- Hence $|G|/deg$ is an algebraic integer which, since rational, is an ordinary integer.

Structure constant formula

- If we multiply two conjugacy-class sums together, the result is a conjugacy class sum.
- How this breaks up is visible in the table of central characters.
- We can use column orthogonality to find out numerically how it breaks up.

How many triples with c.d.e=1?

- Central character is $H(c)\chi(c)/deg$
- Multiply two of these (c,d), convert back to character value and take the (column) inner product with a third class (e) we get that the e class sum occurs in the product of c and d class sums . . .
- $\Sigma[H(c)\chi(c)/deg.H(d)\chi(d)/deg.\chi^{¢}(e).deg/H(e)/C(e)]$ times. $= \Sigma[H(c)\chi(c)/deg.H(d)\chi(d)\chi^{¢}(e)/|G|$
- Number of triples from c,d,e with product 1 is $H(c).H(d).H(e)/|G|.\Sigma[\chi(c).\chi(d).\chi(e)/deg]$

Congruence

- Congruence properties basically arise through restriction.
- For example the values on an element of order 2 are congruent to the degree
- Because they are in the group of order 2

1 1

1 -1

Congruence to p' part

- In the character table of a cyclic group of order $p^{\alpha}.r$, if x has order p^{α} and y has order r, the character on xy is the character on y times z, where z is a p^{α} root of 1.
- The difference is therefore the character value on y times (1-z).
- The p^{α} power of (1-z) is clearly divisible by p (consider p odd and p even separately)

Congruences

- Often in particular cases more powerful (but often more complicated) congruences can be deduced by restricting to other subgroups.
- Things like $\chi(2A) - 2\chi(4A) + \chi(1A)$ is divisible by 8.

Formula for square roots.

- The |G| elements g^2 is in the centre of the group algebra. Its central character is $[\Sigma_g \chi(g^2)]/\deg(\chi)$
- If a class h occurs s times in this, then each element of the class has s square roots. But by column orthogonality s =
- $\Sigma_\chi\{\chi(h).[\deg(\chi)/H(h)]*[\Sigma_g \chi(g^2)/\deg(\chi)]\}/C(h)$
- $= \Sigma_\chi\{\chi(h).\Sigma_g \chi(g^2)\} / H(h)*C(h)$
- $= \Sigma_\chi\{\chi(h). \Sigma_g \chi(g^2)\}/|G| = \Sigma_\chi\{\chi(h). \mathrm{ind}(\chi)\}$

Properties of character tables

1. Table is square
2. Column orthogonality
3. Row orthogonality
4. Indicator +1, 0 or -1 (+,o,- in *Atlas*)
5. Congruent (mod p) to p-part
6. Structure constant formula
7. Central characters are algebraic integers
8. Degrees divide the group order.
9. Characters characterise representations
10. Formula for number of square roots

Representations – Theory and Practice – Lecture 5

Application examples of character theory proving things about groups

No simple group order $p^\alpha q^\beta$ (Burnside)

Any simple group order 4.p.q is A5.

Only finitely many simple groups with a given involution centralizer

Sketch of Burnside's $p^\alpha q^\beta$

- Central characters H(c).χ(c)/degree can have a hard time being algebraic integers
- Especially if H(c) is coprime to the degree, so provides no "assistance".
- In this case either χ(c) is zero or a scalar
- If H(c) is a prime power, orthogonality with the degree shows that the scalar case, true for the trivial character, must happen again, so group cannot be simple.
- Groups of order $p^\alpha q^\beta$ must have such a class.

Special case of key lemma.

- Suppose first that χ(c) an integer and the class size H(c) is coprime to the degree.
- H(c).χ(c)/degree must be an integer, and so χ(c) must be divisible by the degree.
- Being the sum of roots of 1, this can only happen if the matrix is the scalar 1 or -1.
- In either case the element is in the centre of whatever the matrices actually represent.

Burnside $p^\alpha q^\beta$ - χ(c) arbitrary.

- Suppose the class size H(c) is coprime to the degree d. There are therefore integers r and s such that r.H(c) + s.d = 1.
- ψ(c) = H(c).χ(c)/d is an algebraic integer
- r.ψ(c)+s.χ(c)=(χ(c)/d).[r.H(c)+s.d]=χ(c)/d is therefore an algebraic integer.
- If not a scalar, χ(c)/d and all its algebraic conjugates are less that 1 in absolute value.
- Their product is an ordinary integer, so 0.

What does this tell us?

- If a class is coprime to the degree, either the character value is zero, or the matrix is a scalar, so in the centre of whatever the matrices actually represent.
- For a simple group, the latter case can only happen for the trivial representation.

Lemma

- A simple group cannot have a conjugacy class c with $H(c) = p^{\alpha}$ (p prime)
- For otherwise all the non-trivial characters with $\chi(c)$ non-zero would have degree divisible by p.
- So the column orthogonality between the class and the degree would be 1 mod p
- But it has be zero.

Groups of order $p^{\alpha}q^{\beta}$ are solvable

- Now let G be a group of order $p^{\alpha}q^{\beta}$
- A central element of the Sylow-q subgroup must centralize q^{β} at least, so have a class size which is a power of p.
- So cannot be simple.
- Normal subgroup and quotient are solvable by induction.

Simple groups of order 4.p.q

- Centralizer of involution 2A must be order 4, else the class size would be a power of a prime.
- Character values 1,1,1,-1 or 1,1,-1,-1.
- #(2A,2A,2A) must be zero or |G|/2.
- Try to get character table in the 4 cases.
- G is A5.

4.p.q – 2A centralizer order 4

- Now let G be a group of order 4.p.q, where p and q are distinct odd primes.
- A central involution of the Sylow-2 subgroup must have centralizer of order 4, since if it centralized an element of order p (or q), there would be q (or p) elements in its class.

4.p.q - 2A character values

- Must be integers, and the sum of the squares is 4. There is a 1 (the trivial character) but the rest cannot all be 1 (nor all -1) by orthogonality with the degree column.
- Hence the non-zero character values on 2A must be (1,1,-1,-1) or (1,1,1,-1).

4.p.q – #(2A,2A,2A) of product 1

- If three involutions have trivial product, they generate a Klein 4-group. Since the centralizer of 2A is of order four, it cannot be in more than one such subgroup. Either there are none, or the first 2A can be chosen from the class (size |G|/4) and there are precisely two ways to complete it.

Four cases

- (1) 1 1 1 -1 #(2A,2A,2A)=0
- (2) 1 1 1 -1 #(2A,2A,2A)=|G|/2
- (3) 1 1 -1 -1 #(2A,2A,2A)=0
- (4) 1 1 -1 -1 #(2A,2A,2A)=|G|/2

(1) 1 1 1 -1 #(2A,2A,2A)=0

1A	2A
1	1
a	1
b	1
a+b+1	-1

$1 + 1/a + 1/b - 1/(a+b+1) = 0$?
No way! It is obviously positive

(2) 1 1 1 -1 #(2A,2A,2A)=|G|/2

1A	2A
1	1
a	1
b	1
a+b+1	-1

$\Sigma[\chi^3/d]=\#_3.C_3/|G|^2=32/|G|$
$1+1/a+1/b-1/(a+b+1)=32/|G|$
LHS ≥ 1 so |G| ≤ 32. one of a or b is 1, as degree squares ≤ 32. Linear character so not simple.

(3) 1 1 -1 -1 #(2A,2A,2A)=0

1A	2A
1	1
a	-1
b	-1
a+b-1	1

$1 - 1/a - 1/b + 1/(a+b-1) = 0$?
a or b must be 1 to get this down (all odd).

(4-1) 1 1 -1 -1 #(2A,2A,2A)=|G|/2

1A	2A
1	1
a	-1
b	-1
a+b-1	1

$1 - 1/a - 1/b + 1/(a+b-1)=32/|G|$
a and b odd so at least 3 so LHS ≥ 1/3. Hence |G| is at most 96 so a+b-1 ≤ 9.

(4-2) 1 1 -1 -1 #(2A,2A,2A)=|G|/2

1A	2A
1	1
a	-1
b	-1
a+b-1	1

a+b-1 ≤ 9, |G| = 32/[1-1/a-1/b+1/(a+b-1)]

(a,b) is (3,3), (3,5), (3,7), (5,5)

|G| (3,3) 60 [or (5,5) 45 not 4.p.q!]

Get some more character table

60	**4**	*3*		
1A	**2A**	**3A**	**5A**	**. . .**
1	**1**	**1**	**1**	
3	**-1**	*0*		
3	**-1**	*0*		
5	**1**	*-1*	*0*	. . .
4	*0*	*1*		

Can readily fill in the rest.
3 centralizer must be 3, since class size not a power of 2
there is no element of order 6
Already have at least 2 (on 1 and 5) on 3A so need one degree 4 to make degree squares add up and 1A 3A column orthogonality

The degree 5 already has norm 1 so must be zero on remaining classes. Hence (2A.3A.5A) not zero so G must have A5 = <T,S : T^2=S^3=$(ST)^5$=1> as a subgroup.

G is isomorphic to A5

	60	**4**	**3**		
	1A	**2A**	**3A**	**5A**	*5B*
+	**1**	**1**	**1**	**1**	*1*
+	**3**	**-1**	**0**	*-b5*	*
+	**3**	**-1**	**0**	*	*-b5*
+	**5**	**1**	**-1**	**0**	*0*
+	**4**	**0**	**1**	*-1*	*-1*

1A has 16 square roots so all Indicators must be +. No element of order 4 so must be 2 classes of element order 5. 3A.5AB column orthogonality gives values on 4. Indicator + so values of 3 on 5A real. Norm and inner product then gives values by solving a quadratic equation,

Reducing 3 mod 2 real odd dimensional so has 1 as constituent. Hence G in L2(4). Reduce it mod 5 and it is in O3(5) which is L2(5). And so on. This is A5!

Simple group has bounded order given involution centralizer

- "Usual" proof involves counting pairs of involutions.
- Character-theoretic proof also indicates how to actually find the group.

Involution centralizer theorem.

- Given an involution centralizer C, disjoin x = how many other involutions of C are in the same conjugacy class in G, so #(2A,2A,2A)=x.|G|/|C|
- Now disjoin all ways that the centralizer order is the sum of squares.
- Either the degree of some character is small, or the group order is close to $x.C^2$.
- (Can reduce mod p so small degree => small)

Representations – Theory and Practice – Lecture 6

Induced Representations

Induced representations

- John Thompson once started a lecture . . .
- "Let G be a finite group and H a subgroup of G . . . That sets up a tension".
- I feel that is an appropriate comment about induced representations.

Basic facts

- Given a representation of a subgroup H, there is a corresponding induced representation of G.
- It is well-defined, and its character can be computed.
- Induced representations are important!

Other facts

- Works over anything even resembling a ring!
- Induction is transitive – induce up from a subgroup of a subgroup and whether you go via the middle one makes no difference.
- Frobenius reciprocity – "inner product" between a representation of H and a representation of G is the same whether you restrict one or induce the other.
- Induce a decomposable (reducible) and you get a decomposable (reducible)

Vertices, Sources

- For any representation σ of G, it may or may not be a direct summand of some representation induced from H.
- There is a p-subgroup V(ertex) of G such that σ is such a direct summand if and only if V is contained in (some conjugate of) H.
- There is then a representation ρ(Source) of H such that σ is a summand of ρ↑.

Imprimitive representations.

- Can start with a representation σ of a group G.
- Suppose the space on which σ acts is the direct sum of subspaces $[V]_i$ that σ(g) permutes. We call such a representation "imprimitive".
- The (setwise) stabilizer in G of M_1 is a subgroup H acting (as ρ) on $[V]_1$
- This process can be reversed.

Choose X a set of coset reps

- So that G = H.X – every element of G has a unique representation as h.x.
- Given an element g of G, we then, for each x in X, find this unique expression for x.g (as h.x').
- Hence we get two functions
  - ***H***(x,g) the element of h
  - ***X***(x,g) the coset representative

Example G = S3, H=C2.

So G is the set of all permutations on {1,2,3} and H is the set {I , (2,3)}

For X (coset reps) I chose x_1=I, x_2=(1,2) and x_3=(1,3,2). (where does 1 go?)

Let g be the permutation (1,3).

$x_1.g$= (2,3). x_3 so $\underline{\boldsymbol{H}}(x_1,(1,3))=(2,3)$; $\underline{\boldsymbol{X}}(x_1,(1,3))=x_3$

$x_2.g$= (2,3). x_2 so $\underline{\boldsymbol{H}}(x_2,(1,3))=(2,3)$; $\underline{\boldsymbol{X}}(x_1,(1,3))=x_3$

$x_3.g$= (2,3). x_1 so $\underline{\boldsymbol{H}}(x_3,(1,3))=(2,3)$; $\underline{\boldsymbol{X}}(x_1,(1,3))=x_1$

Axioms of wreath systems

Since $x.(g_1.g_2)=(x.g_1).g_2$ a and $x.g = \underline{\boldsymbol{H}}(x,g).\underline{\boldsymbol{X}}(x,g)$ and as we started with a group, $x.(g_1.g_2) = (x.g_1).g_2$

- Hence $\underline{\boldsymbol{H}}(x,g_1 g_2)=\underline{\boldsymbol{H}}(x,g_1).\underline{\boldsymbol{H}}(\underline{\boldsymbol{X}}(x,g_1),g_2)$
- and $\underline{\boldsymbol{X}}(x,g_1g_2) = \underline{\boldsymbol{X}}(\underline{\boldsymbol{X}}(x,g_1),g_2)$
- We can call such a pair of functions a wreath system over H.

Wreath systems are not more general

- It can readily be shown that every wreath system can be constructed out of a group and a subgroup in the obvious way . . .
- The group $\underline{\boldsymbol{H}}$ in the wreath system may be a homomorphic image of the subrgroup, but this changes very little since the representation we induce may just as well represent a homomorphic image.

ρ represents H, ρ↑ represents G

- Given any representation ρ of H, can make the induced representation ρ↑ of G
- Take the direct sum of (H:G) spaces on which ρ acts, indexed by the elements of X – the coset representatives. If v is a vector on which ρ acts, denote by $[v]_i$ the one in the i'th component.
- If $x_i.g=h.x_j$ define $[v]_i.\rho\uparrow(g) = [v.\rho(h)]_j$
- Or in full . . . $[v]_x.\rho\uparrow(g) = [v.\rho(\underline{\boldsymbol{H}}(x,g))]_{\underline{\boldsymbol{X}}(x,g)}$

Basic facts about induced representations

- This is a representation of G
- It does not depend on the choice of coset representatives.
- $\chi\uparrow(g) = \Sigma D_h \chi(h)$
  Where the sum is over classes h of H conjugate in G to g, and D_h is the index of $C_H(h)$ in $C_G(g)$.

This ***is*** a representation (short version)

- Reminder . . . $[v]_i.\rho\uparrow(g) = [v.\rho(h)]_j$
- Suppose $x_i.g_1=h_1.\ x_j$ and $x_j.g_2=h_2.\ x_k$
- Then $x_i.g_1g_2 = h_1h_2x_k$
- $[v]_i.\rho\uparrow(g_1)\ .\ \rho\uparrow(g_2) =[v.\rho(h_1)]_j\ \rho\uparrow(g_2)$
- $=[v.\rho(h_1)\rho(h_2)]_k =[v]_i.\rho\uparrow(g_1g_2)$

This ***is*** a representation (long version).

- Reminder . . . $[v]_x.\rho\uparrow(g) = [v.\rho(\underline{\boldsymbol{H}}(x,g))]_{\underline{\boldsymbol{X}}(x,g)}$
- $[v]_x.\rho\uparrow(g_1g_2) = [v.\rho(\underline{\boldsymbol{H}}(x, g_1g_2))]_{\underline{\boldsymbol{X}}(x,g1g2)}$
- $[v]_x.\rho\uparrow(g_1)\rho\uparrow(g_2)$
  $= [v.\rho(\underline{\boldsymbol{H}}(x,g_1))]_{\underline{\boldsymbol{X}}(x,g1)}.\rho\uparrow(g_2) =$
  $[v.\rho(\underline{\boldsymbol{H}}(x,g_1)).\rho(\underline{\boldsymbol{H}}(\underline{\boldsymbol{X}}(x,g_1),g_2))]_{\underline{\boldsymbol{X}}(\underline{\boldsymbol{X}}(x,g1),g2,)}$
- Reminder
- $\underline{\boldsymbol{H}}(x,g_1g_2)=\underline{\boldsymbol{H}}(x,g_1).\underline{\boldsymbol{H}}(\underline{\boldsymbol{X}}(x,g_1),g_2)$
- $\underline{\boldsymbol{X}}(x,g_1g_2) = \underline{\boldsymbol{X}}(\underline{\boldsymbol{X}}(x,g_1),g_2)$

Long versions omitted

- Perhaps I am just lazy . . .
- Or perhaps I am just expecting you to be lazy
- But doing induced representations the long way is just too much like work.
- Exercises for the reader coming up!
- The following two results are a lot of slog and no real understanding would result.

Change of coset representatives

- Reminder . . . $[v]_i.\rho\uparrow(g) = [v.\rho(h)]_j$
- Suppose we instead choose $y_i = h_i.x_i$
- If $x_i.g = h.x_j$ then $y_i.g = h_i.x_i.g = h_i.h.x_j$ $= h_i.h.h_j^{-1}x_j$ so all we have done is conjugate our representation by $\mathrm{diag}[\rho(h_i)]$.

The induced character value

The induced character $\chi(z)$ is clearly
$\Sigma\Psi(x^{-1}.z.x^{-1})$ over coset reps x.

- (with the convention that $\Psi(g)=0$ if g is not an element of H)
- But as all of G is H.X we have
- $\chi(z) = \Sigma\Psi(g^{-1}.z.g^{-1})/|H|$ (same convention)

Or $\chi\uparrow(g) = \Sigma D_h \chi(h)$

- Only need look at $x_i.g = h.x_i$ (same i) as otherwise the matrix $\rho(h)$ is off the diagonal so does not contribute to the trace.
- But then $x_i.g.x_i^{-1} = h$
- So can take g=h (they have the same character)
- Cosets conjugating h to an H-conjugate are clearly precisely those containing a commuting element.
- So we may take the x_i as coset representatives of $C_H(h)$ in $C_G(h)$

Next week.

- We now have the fact that if χ is a character of H, then $\Sigma D_h \chi(h)$ is a character of G
- This can be applied to prove further theorems about groups.
- In particular, Frobenius' theorem – in a transitive group where only the identity fixes 2 or more points, the fixed-point-free elements form a (normal) subgroup.

Representations – Theory and Practice – Lecture 7

Generalized characters, lattices and embedding them

Induced Characters and TI sets.

Remark about characters.

- There are three sets of characters we are often interested in.
- The irreducible characters
- The "genuine" characters – the characters of representations – non-negative integral linear combinations of irreducible characters
- The "generalized" characters – arbitrary integral linear combinations of irreducible characters.

Generalized characters

- It can be useful to work with generalized characters. It can often happen that you get a generalized character of small norm and can figure out what linear combination it is.
- In particular if a generalized character has norm is 1 and the degree is positive it is genuine after all.
- This is our first lattice embedding theorem!

Generalized characters are a lattice

- The span of any set of generalized characters form a free Z-module with a positive definite integral quadratic form.
- I call that a lattice.
- Indeed it is a sublattice of 1^n
- So given any set of generalized characters they must embed somehow into 1^n

Example lattice

Suppose we have three characters whose inner product matrix is . . .

```
 2 -1
-1  4
```

Ignoring sign, we see that the 2 is two irreducibles, and the 4 has odd inner product with something so cannot be twice an irreducible. We have 11000 and -10111!

D4

Suppose we find generalized characters whose inner product matrix is D4. Then

```
 2 -1 -1 -1
-1  2  0  0
-1  0  2  0
-1  0  0  2
```

however this is embedded into 1^n, some pair from the last 3 characters adds up to twice an irreducible. Hence one can disjoin three cases and halve one of them.

E6 does not embed

If you find 6 generalized characters with the inner product matrix of E6 . . .

```
 2 -1  0  0  0  0   Then you have a
-1  2 -1  0  0  0   contradiction!
 0 -1  2 -1  0 -1   From the D4, every pair has
 0  0 -1  2 -1  0   odd inner product with
 0  0  0 -1  2  0   something so cannot be
 0  0 -1  0  0  2   halved.
```

Future hint - The Green Ring

- Actually we can form the "generalized indecomposables" in the modular case.
- A representation is a positive integral linear combination of indecomposables (Krull-Schmitt!)
- We can also form the abstract thing – arbitrary integral linear combinations of indecomposables.
- Tensor product gives us a multiplication on this, and the resulting ring is called the Green Ring.

Thompson's Tension

- Suppose we are interested in groups G containing S3.
- We know the character table of S3, so if we knew the order of the centralizers in G of the three classes of elements in S3 . . .
- We could form the induced characters and check that they are sensible.

Representations induced from S3

6	2	3
1A	2A	3A
1	1	1
1	-1	1
2	0	-1

6a	2b	3c	
1A	2A	3A	rest
a	b	c	0
a	-b	c	0
2a	0	-c	0

For example, restricting the first induced character to S3 and taking the inner product with the second character of S2, we get that a/6–b/2+c/3 is an integer.

Frobenius group S3 example

- Now suppose we have a Frobenius permutation group where the point stabilizer is S3, and the non-trivial elements of S3 fix *only* one point.
- Hence b=c=1 in the previous example.
- We can therefore start a character table of G

So G has an S3 quotient!

[1]	[3a]	[2a]	[a-1]	class sizes
6a	2	3	….	centralizers
1A	2A	3A	rest	
a	1	1	0	A induced
a	-1	1	0	B induced
2a	0	-1	0	C induced
1	1	1	1	D trivial character
2	0	-1	2	C + 2.D – 2.A

Frobenius groups in general

If a permutation group is transitive and every non-trivial element fixes at most 1 point, then the identity along with the fixed-point-free elements form a normal subgroup.

Sketch of proof

- Let H be the point stabilizer. If H=1 there is nothing to prove.
- Otherwise let X be the generalized character X=(permutation-trivial)
- Then for each irreducible character of H (of degree d) induce it up and subtract d.X from it.
- The resulting character is a generalized character of norm 1 positive degree so irreducible. Its value on the degree and the fixed-point free elements are equal.
- The identity and fixed-point-free elements are the only elements in the kernel of all these representations.

illustration

H the point stabilizer of index n

1	**(n-1)H**	**(n-1)**	
1	**h**	**f**	
1	1	1	Trivial character
n	1	0	Permuation character
n-1	0	-1	X = permutation-trivial
n.d	$\chi(h)$	0	induce from d $\chi(h)$ on H
d	$\chi(h)$	d	norm is 1 as it is on χ

Frobenius groups are TI sets

- What we *really* use is that the non-trivial elements of H form a TI set – a set T of elements of G such that $g^{-1}.T.g$ is either T or is disjoint from T.
- The set of g where $g^{-1}.T.g = T$ is H – the group we use to induce up from.
- If this is just T along with the identity, we have the Frobenius group case.

Trivial intersection sets

- Let T be a TI-set – a set of elements such that for all g in G either g normalizes T or $g^{-1}Tg$ has no element in common with T.
- Let H be the normalizer of T.
- Inducing up a generalized character of H that is zero outside T leaves the character value unchanged, for H contains every element that conjugates t into T.
- $\chi\uparrow(t)=\Sigma\ D_h\ \chi(h)$ but there is only one h with $\chi(h)$ non-zero, and for that h, $D_h=1$

Trivial Intersection - 2

- Now take the set of generalized characters of H that are zero outside T. This is clearly a lattice.
- Inducing up all those characters retains their norms and inner products since the character values and centralizers are unchanged.
- So we can try to embed them into 1^n.

Exceptional characters.

- Suppose further that there are e>1 characters of H of the same degree that are zero outside T (except on 1)
- Then G also has e characters [the **exceptional** characters] of the same degree whose differences are (+/-) the induction of the H-character differences.
- Because the lattice A_n only embeds in 1^n in one way.

Examples of TI sets

- Given any z, the elements x such that x^s generates <z> [for some integer s] form a TI set.
- The normalizer H of <z> is the normalizer of the TI set.
- This is particularly useful where z is an involution whose centralizer (H above) is known.

Involution centralizers again

- This is usually a good place to start given an involution centralizer $C_G(t)$
- Take the set of generalized characters of $C_G(t)$ zero on elements that do not power to t.
- Take the inner product matrix and try to find all the ways of embedding that in 1^n

Powerful stuff

- One wonders how anyone ever did any finite group theory without representation theory.
- More specifically it becomes clear that, to study groups in a classification setting, trying to get facts about the character table is a powerful method.

Richard Brauer

- The methods described so far are so powerful that even a minor extension to them can have major implications.
- This was the original reason for studying modular representations, but post-classification there is more interest in the representations themselves.
- I will gradually shift emphasis in this direction.

Representations – Theory and Practice – Lecture 8

- Wedderburn's theorem
- Modular character theory – what is knowable?
- Summary of initial results that get you going
- Overview of modular representation theory.

Wedderburn's theorem

- A finite skew-field [+ is an abelian group, * (except 0) is a group, and distributivity on both sides] is a field.
- Its order is a power of a prime (take the subring generated by 1 – must be a vector space over that).
- BUT in multiplicative group all centralizers are subrings (not just subgroups) and that is just to great a burden to bear.

Proof 1 – first half

- Take the smallest counterexample. Then every sub-skew-field is a field by induction.
- The multiplicative group has order p^n-1.
- The every non-central element generates (under + and *) a proper sub-skew-field so generates a field
- Hence every non-central element is in a cyclic group whose order is p^m-1 for some n.

Proof 1 using Zsigmondy's theorem

- Unless $p^n=64$, there is a prime divisor q of p^n-1 that does not divide p^m-1 for any $m<n$.
- If $p^n\neq64$ take x an element of order q in our skew-field (there is one by Sylow's theorem)
- It generates a finite field whose order must be p^n-1 since no smaller power will do.
- If $p^n=64$: groups of order 63 have a commutative Sylow-3 subgroup of order 9 which still cannot generate less than 64.

Proof 2 by counting elements – first half

- Looking at the multiplicative group . . .
- The centre must have order $q-1=p^a-1$.
- The whole group has order q^n-1
- Let x be a non-central element. Then its centralizer is order q^m-1 for $1<m<n$ and indeed m divides n as we have a vector space over the centralizer.

Total number of elements

- Total number of elements is the sum of the conjugacy classes
- $q^n-1 = (q-1) + \Sigma(q^n-1)/(q^m-1)$
- Let $r = \Psi(q)$ where Ψ is the n^{th} cyclotomic polynomial. Then r divides q^n-1 and every $(q^n-1)/(q^m-1)$ so also divides q-1.
- But r is greater than q-1. [product q-z over primitive n^{th} roots of 1, each bigger than q-1 in absolute value]

Modular character theory – what is knowable

- The irreducible representations. Not always easy to find, but they, and their properties, are there to be found.
- The indecomposable representations are, in general, not knowable. If you knew all the representations for the Sylow-p subgroup that'd be a good start.
- There is considerable interplay between the representations mod p and the p-adic representations.

To get going you need

- Wedderburn - Finite division rings are fields
- Commuting matrices, Homs and p-adic numbers all play a large role
- Krull-Schmidt – Direct sum decomposition is well defined
- Mackey – <induce then restrict> is <restrict then induce> from intersections of conjugates

Overview of modular representation theory.

- What can you induce up from where to get your representation as a summand?
- First understand p-groups (impossible)
- Then go to normaliser of p-group
- Then go to the whole group.

- If you understand the start (small p-group or trivial representation) you can succeed.

Tools of study

- Blocks and defect groups.
- DimHom Inner product
- Irreducibles and projective indecomposables
- Theorems about induction and restriction
- Vertices and sources
- Relationship between char 0 and p
- Cyclic defect and trivial source
- Species, characters

Blocks and defect groups

- For any representation, add up all the elements of any conjugacy class and you get something that commutes
- The eigenspaces decompose your representation
- They are the reduction mod p of the central characters
- So look at the central characters mod p and see how your group decomposes.

DimHom inner product

- Given any two representations, the dimension of the set of matrices with AX=XB is the DimHom inner product.
- In some cases – in particular summands of permutation representations - you can calculate it.

Irreducibles and projective indecomposables

- *Decompose* the regular representation.
- The summands are in 1-1 correspondence with the irreducibles, which are the unique irreducible quotient.
- The DimHom inner product picks out the irreducible composition factors of any representation

Theorems about induction and restriction.

- Restrict to the Sylow-p subgroup and induce back up, and your representation is a summand.
- Mackey - Induce then restrict is the same as restrict to intersections and then induce
- Green – induce absolutely indecomposable from normal subgroup of index p and the result is absolutely indecomposable

Characteristic 0 and characteristic p relationships

- P-adic numbers go part way from complex numbers to finite fields.
- Given a charactersitic 0 representation, can always reduce mod p.
- Summands of permutation modules, and in particular projective indecomposables, always lift.

Vertices and Sources

- Restrict your representation to the Sylow-p subgroup and decompose
- Some summand of that, induced up again, gives you your original representation as a summand.
- The smallest p-group for which you can do this is called the vertex
- And the representation of the vertex you induced is called the source
- Cyclic vertex and trivial source are two areas that one can study and make progress.

Cyclic vertex and trivial source

- The representations of the ***cyclic*** p-groups are easy to understand – Jordan Blocks.
- This makes the representations with cyclic vertex comprehensible
- The trivial representation of a p-group can be induced up and the result decomposed.
- These decompositions lift to characteristic zero, enabling computations.

Modular characters give irreducible constituents

- If you know the eigenvalues of all the elements, you know the constituents.
- The eigenvalues on the p' elements are all that matter.
- We can therefore get a square modular character table as a way of displaying the eigenvalues. Examples and definitions follow.

Example – A5 mod 11

	60	4	3	5	5
p power		A	A	A	A
p' part		A	A	A	A
ind	1A	2A	3A	5A	5B
+	1	1	1	1	1
+	3	-1	0	-b5	*
+	3	-1	0	*	-b5
+	4	0	1	-1	-1
+	5	1	-1	0	0

Species and characters

- A ***species*** is a map s from representations to the complex numbers such that
  $s(\rho+\sigma) = s(\rho) + s(\sigma)$ (direct sum)
  $s(\rho \times \sigma) = s(\rho) \times s(\sigma)$ (Tensor product)
- Species of subgroups are species
- Species obtained by restricting to p' subgroups are called the ***Brauer characters***.

P-adics

- The p-adic representations are characteristic zero, so the same as the ordinary ones
- We can write them in the p-adic integers (principle ideal domain) and so reduce mod p
- Some reduction is indecomposable!
- If p is coprime to the group order (as in A5 mod 11), this implies irreducible mod p.

Sqrt(5) in the 11-adics

- $4^2=5 \pmod{11}$ $7^2=5 \pmod{11}$
- $(4+11a)^2=(16+11.8a) \pmod{121}$
- $1+8a=0 \pmod{11}$ $a=4$
- $48^2=5 \pmod{121}$ . . . . . .
- 5 has two square-roots in the 11-adic numbers.
- So when we look at the 3-dimensional characters of A5 mod 11, we would like to know what we mean by sqrt(5).

Brauer's definition

- Restrict to a cyclic p' element
- Look at the eigenvalues
- Lift those eigenvalues to the comples numbers in a consisent way
- Add them up as complex numbers

Irreducibles of A5 mod 2

	60	3	5	5
p power		A	A	A
p' part		A	A	A
ind	1A	3A	5A	B*
+	1	1	1	1
–	2	-1	b5	*
–	2	-1	*	b5
+	4	1	-1	-1

Projectives indecomposables of A5 mod 2

60	2	3	5	5
p power	A	A	A	A
p' part	A	A	A	A
1A	2A	3A	5A	B*
12	0	0	2	2
8	0	-1	-b5	*
8	0	-1	*	-b5
4	0	1	-1	-1

Representations – Theory and Practice – Lecture 9

Homs and endomorphisms

Krull-Schmidt

Hom

- Given any two representations A and B of the same group, we can form Hom(A,B) = { X : XB = AX }
- The dimension of this space is called DimHom(A,B), and this is an inner product on the set of representations (and indeed on the set of generalized representations)

Endomorphisms

- Hom(A,A) is of great importance. Such matrices are called endomorphisms, and the set End(A) is closed under both addition and multiplication.
- If A is irreducible, End(A) is a division ring.
- If A is indecomposable, End(A) is a *local ring*.
- It is actually this property that leads to Krull-Schmidt.

Confession

- I have tried to work out exactly when this proof works for modules over an arbitrary ring.
- I have not entirely succeeded! ☹
- In this course, we are interested in matrix representations over fields, (i.e. group rings over fields) and here there is no problem.
- Please excuse my partial generalizations. They confuse me! In particular the use of the D.C.C. is not made entirely explicit.
- I think Krull-Schmidt is true for representations over a local ring with DCC – e.g. mod 4.

Overview of Krull-Schmidt

- (personal terminology for this lecture only) A representation over a field is "pretty" if the sum of two singular endomorphisms can't be non-singular.
- The decomposition of a module as a direct sum of "pretty" modules is unique.
- All indecomposables over fields are pretty.

When does Krull Schmidt work?

- Does NOT work over the integers. For C23 has three non-isomorphic irreducible representations of dimension 22 – A, B and C, say. B+B=A+C.
- Does not work mod 6. 2 and 3 are independent, and you can move mod 3 stuff to a different mod 2 summand.
- I am pretty sure it works mod 4, though.

Fitting's Lemma

- Over a field, a square matrix is either invertible or singular.
- A singular matrix all of whose eigenvalues are the same is nilpotent (look at the Jordan Blocks).
- More generally if you have both Chain Conditions you can power up a matrix until its image stabilizes and the space is now the direct sum of kernel and image. This works mod 4.
- It is this that fails for the ordinary integers. The matrix [2] is neither invertible nor nilpotent.
- It also fails mod 6, where the image may not be free. Again the matrix [2] provides an example.

The "pretty" property of indecomposables.

- Consider the set of endomorphisms of an indecomposable over a field.
- If h1=h2+h3, h1 invertible and h2 singular, then h3 is invertible.
- Otherwise multiply by the inverse of h1 and we get 1=s1+s2 where s1 and s2 are singular.
- $s1^n=0$ for some n as otherwise we get a decomposition using the eigenvalues of s1.
- Now $1=1^n=(s1+s2)^n=s1^n+s2$(some stuff)
- So s2.(some stuff) = 1

Unique decomposition

- I call ***pretty*** any representation where every endomorphism is either invertible or is singular (v.e=0) and there are no two singular endomorphisms s1 and s2 with s1+s2 invertible. As we have seen, indecomposables over fields are pretty. Clearly decomposable representations are **not** pretty (take the two projections).
- Mod 6 we have 2+3=5 – not a pretty sight.

Some properties of pretty modules

- If you add any number of singular endomorphisms the result is still singular.
- Benson implicitly says that if a module has a pretty decomposition, then all decompositions are pretty. I cannot follow his argument and am unsure whether it is in error or just that I cannot follow it.
- All I can show is that two decompositions that are *both* pretty are the same.

The two steps

- Given two direct sum decompositions into pretty modules, we need to show that . . .

1. An indecomposable appears on both lists
2. There is an isomorphism that takes one to the other.

I have got each step onto one slide, which makes it easier to keep everything up.

I am taking them in the opposite order.

Step 2 overview

- True in great generality.
- **If we can find an isomorphism** between Q'+X and Q+Y that takes vectors of Q' to tα+tφ where α is an *isomorphism* from Q' to Q, and φ is an arbitrary map into Y, **then we can get rid of φ and find an isomorphism that takes Q' to Q.**

Step 2 proof.

Suppose Q' and Q are isomorphic by an isomorphism α, and Q'+X is isomorphic to Q+Y by an isomorphism β such that for t in Q', $t\beta = t\alpha+t\varphi$ with $t\varphi$ in Y, then there is an isomorphism μ from Q'+X to Q+Y taking Q' to Q

Proof. Let q and y be the projections of Q+Y onto Q and Y respectively. **Define $\mu = \beta(1-q\alpha^{-1}\beta y)$.** Then μ is an isomorphism, for both Q and Y are in its image. For Q, notice that for t in Q', $t\mu=t\beta-t\beta q\alpha^{-1}\beta y=t\beta-t(\alpha+\varphi)q\alpha^{-1}\beta y=t\beta-t\alpha\alpha^{-1}\beta y = t\beta-t\beta y=t\beta q=t\alpha$ [so Q'μ=Q] which is clearly onto Q. On the other hand since for t in Y, $tq=0$, $t\beta^{-1}\mu=t(1-q\alpha^{-1}\beta y=t-tq\alpha^{-1}\beta y=t$ hence onto Y [ker=0 can be proved as well, but we do not need it since we are in a field].

Krull-Schmidt

- Let p_i and u_j be two pretty decompositions of the same module. Then they are the same up to order.
- Take the projection idempotents q_i and w_j and *let p_1 be a submodule from either list of greatest dimension.*
- Then since $q_1=q_1q_1=q_1.1.q_1= q_1.\Sigma\, w_j.q_1$ we must have $q_1.w_j.q_1$ non-singular on p_1 for some j since the p_i are pretty. *Since p_1 has the largest dimension*, **w_j is an isomorphism** between p_1 and u_j and now as w_j acts the same as the identity on u_j, step 2 shows that there is an isomorphism taking p_1 and u_j. Taking quotients and using induction completes the proof.

References

- That proof comes from Puttaswamaiah and Dixon – modular representations of finite groups.
- Dornhoff gives a similar looking proof.
- None of them are really intuitive.

Representations – Theory and Practice – Lecture 10

Some facts about the p-adics.

Brauer Characters and Conway Polynomials

P-adic numbers.

- In general, we start with a representation written in algebraic number field obtained from the rationals and roots of unity.
- To get the idea though, I will start with the rationals.
- In either case, you start off by taking the algebraic integers of your field.
- So let's start with the ordinary integers.

Ordinary p-adic integers.

- Take the ordinary integers and choose a prime (11, say) and reduce modulo p^n for increasing n.
- This gives a sequence of rings with a homomorphism from each to the previous.
- e.g. mod 11, 121, 1331, 14641 etc.
- The p-adic integers are the unending sequences of elements, one from each of these rings with each having the previous as its homomorphic image. Uncountable ☹

Localization

- In my opinion, reduction mod p is easier done by redefining the "integers" of an algebraic number field to be anything whose denominator is coprime to p.
- This makes a P.I.D. and allows for reduction.
- But we sometimes need [Hensel] to argue that we never need to stop when finding an element modulo higher and higher powers of a prime and therefore there is a characteristic 0 thing that reduces to it.

Examples

- For example we may choose 5 from every ring (mod 11, mod 121, mod 1331 etc.)
- We call this sequence 5.
- As we saw on Monday, in this ring, 5 has a square root.
- The second term is 48 (mod 121)
- Hence there are some irrational numbers that are 11-adic integers.

The sequences of rings you get depends on where you start. p=2

- For example you might take $a + b\omega$ for a,b integers, $\omega^3=1$. In that case the first ring is the field of order 4.
- Or you might take $a + bi$ for a,b integers and $i^2=-1$ and p=2. You have to use the ideal (1+i) which squares (as an ideal) to the ideal generated by 2.

Properties of p-adic integers

- They form an integral domain. Hence one can form the field of fractions.
- The integers form a principle ideal domain.
- Theorem – any representation over the field of fractions of a principle ideal domain can be written over the domain, eliminating the denominators.

Why representations in integers?

- Let D be principle ideal domain. Then any finitely generated torsion-free module is free (has a D basis)
- Given a representation in the field of fractions of D, take any vector and consider the D-span of all its G-images. This is a finitely generated torsion-free D-module so has a D basis.
- Now the representation is written over D.

Fintely generated torsion free

- Take vectors as basis elements until you get a relation.
- So $d_n.v_n = d_1.v_1 + d_2.v_2 + \ldots d_{n-1}.v_{n-1}$
- They cannot all be divisible by d_n
- Find the generator of the ideal generated by d_n and d_1
- Use this to find a new v_1 that spans more than before . . .

P-adics are part of the way to modular

- On one hand they have characteristic zero, so the representation theory is ordinary.
- The issues with irrationalities arises here. Which square-root of 5 do you mean?
- There are division rings, though. For example the quaternions over the 2-adics. Even mod 4 there is no $a^2 + b^2 = -1$

Characteristic p representations.

- A p' element is an element whose order is coprime to p.
- Two representations have the same constituents if and only if every element has the same eigenvalues with the same multiplicity.
- The number of distinct absolutely irreducible representations is equal to the number of p' conjugacy classes.

Eigenvalues depend only on the p' part.

- If p is the characteristic, then a p-element has all its eigenvalues 1. Since any element is the product of its p part and its p' part, and they commute, the eigenvalues are not changed by multiplying by a p-element.
- Can see this by considering Jordan blocks.

Same eigenvalues implies same constituents. - overview

- Frobenius-Schur theorem - you can find an element of the group algebra that has any specified matrix in each irreducible at once. Not proving this today.
- Make it 1 at the top left on one of them gives traces congruent implies multiplicities congruent.
- Induction can do the rest (with care).

Frobenius-Schur theorem.

- Have not found a proof in line with the approach I am taking.
- I will continue to look and hope to give it on Monday.
- Says that you if you choose any matrix independently for each irreducible, you can find a group algebra element that comes to that.

Traces congruent implies multiplicites congruent.

- Make the element of the group algebra that is 1 on some representation. Its trace is implied by the traces of the elements, and measures the multiplicity of that representation mod p.
- Notice that this implies that there is no representation whose trace is zero on every element.

Induction step.

- Now take two representations of minimum degree with different multiplicities of irreducibles but the same eigenvalues on every element.
- Then if there is an irreducible in both, subtract it and you get a smaller counterexample
- Otherwise divide them both by p and you get a smaller counterexample.

Modular Characters

- We therefore need to find a notation for "character" that gives all the eigenvalues, not just the trace.
- Brauer says . . . Choose a multiplicative isomorphism between the roots of unity in characteristic p and the p' complex roots of 1.
- And tabulate the sum of those complex roots of unity on every element.

Brauer characters give the characteristic roots.

- This is a theorem about sets of complex roots of unity – if you know the sum of it and all its powers, you know all the roots of unity.
- Can work out all the symmetric functions (induction on the degree)
- So can work out the polynomial whose roots are your set.

Choosing a Brauer Map

- choose a "consistent" set of irreducible factors C(p,d) of the cyclotomic polynomial mod p for each p,d - an irreducible polynomial for each p,d whose roots have largest order p^d-1 (is "primitive") and such that for each m dividing d, the p^d-1 / p^m-1 power of a root of C(p,d) satisfies C(p,m)
- Can then map a root of C(p,d) to $\exp(2\pi i/p^d-1)$

Good Choice of C(p,d) ?

- I don't think there is a good choice.
- I looked very hard indeed.
- To publish a book of modular characters I had no real alternative but to choose one.
- I gave up and followed Conway's suggestion of using "lexicographically earliest" in the end,

Conway's choice of C(p,d)

- Order the polynomials of degree d lexicographically.
- Actually it is slightly better to negate alternate terms first, so we did – we want to order the roots, not the polynomials.
- Then choose the lexicographically earliest primitive one that is consistent with all smaller degree.
- [Yes, this really is possible]

A proof is in Nickel's PhD thesis

- This is a theorem about finite cyclic groups. If H is a subgroup of G and we say that generators g of G and h of H are consistent if the smallest power of g that is in H is in fact h.
- If you choose generators for some set of subgroups of G closed under intersection that are all consistent within themselves, there is a consistent generator g of G.

Example

- Mod 11, the smallest value of a for which x-a is primitive (i.e. a has order 10) is x-2
- 1,2,4,8,5,10,9,7,3,6.
- Hence the "obvious" complex fifth root of 1 (z5) corresponds to 4.
- b5=z5+(z5)^4 corresponds to 4+3=7
- b5*=(z5)^2 +(z5)^3 corresponds to 5+9=3.
- No-one can confuse 7 and 3, can they?
- This enables us to distinguish the two square roots of 5 in the 11-adics. The positive square root is 4 mod 11.

Tabulation of Conway polynomials

- Much work has been done tabulating them.
- It is very convenient for computer work to have a standard name for elements of finite fields that enables you to get to subfields and larger fields.
- Can get quite hard. Mod 2, it is easy to find the smallest primitive polynomial of degree (say) 61. Just look at the first few and you soon find one.
- But now you want the lexicographically earliest polynomial of degree 122 whose power satisifies your degree 61. You expect to look at about 1,000,000,000,000,000,000 before you find one.

C(11,d) for d ≤ 13

- 11 1 1 9
- 11 2 1 7 2
- 11 3 1 0 2 9
- 11 4 1 0 8 1 0 2
- 11 5 1 0 0 1 0 0 9
- 11 6 1 0 3 4 6 7 2
- 11 7 1 0 0 0 0 0 4 9
- 11 8 1 0 0 0 7 7 1 7 2
- 11 9 1 0 0 0 0 0 0 9 8 9
- 11 10 1 0 0 0 0 7 8 1 0 6 6 2
- 11 11 1 0 0 0 0 0 0 0 0 0 1 0 9
- 11 12 1 0 0 0 1 1 4 2 5 5 6 5 2
- 11 13 1 0 0 0 0 0 0 0 0 0 0 7 9

Representations – Theory and Practice – Lecture 11

Some examples of modular representations.

Extra lecture inserted because I felt that there has been too much theory and not enough practice.

Today we will be tourists. Let me show you around.

Example 0 – the trivial group

- In a sense there are two representations
- [1] and [0]
- We discard the zero "representation" and pretend it doesn't exist yet the trivial representation [1] of every group plays a substantial part. I have no explanation for this!
- Character table for all fields

```
ind  1A
  +   1
```

Example 1 – Cyclic 2 [1 of 2]

- Character table for all primes except 2

```
ind   1A   2A
  +    1    1
  +    1   -1
```

- Character table mod 2

```
ind   1A
  +    1
```

Example 1 – Cyclic 2 [2 of 2]

```
1  1        0  1        1  0
0  1        1  0        1 -1
```

basis regular conjugated

(det = 1)

In the conjugated regular representation, all irreducibles for the rationals visible.

Example 2 – Cyclic 3 [1 of 2]

- Character table for all primes except 3

```
ind   1A   3A B**
  +    1    1    1     (z3)^3 = 1
  o    1   z3   **     Mod 5 needs F25
  o    1   **   z3     Mod 7 F7 will do
```

- Character table mod 3

```
ind   1A
  +    1
```

Example 2 – Cyclic 3 [2 of 2]

```
1  1  1        1  0  0
0  1 -1       -1  1  3
0  0  1        1 -1 -2
```

basis conjugated

(det = 1)

```
1  and  1  3  [=  1  0 (mod 3)
       -1 -2     -1  1         ]
```

Example 3 – S3 [1 of 3]

- Character table for all primes except 2 and 3

```
ind   1A   2A   3A
  +    1    1    1
  +    1   -1    1
  +    2    0   -1
```

- Character table mod 2

```
ind   1A   3A
  +    1    1
  +    2   -1
```

- Character table mod 3

```
ind   1A   2A
  +    1    1
  +    1   -1
```

Normal p-groups

- If G has a normal subgroup whose order is a power of p
- The irreducible representations of G in characteristic p represent it trivially.
- Because any p-group has to fix some non-trivial vectors, which would be an invariant subpace . . . so is the whole space!

Example 3 – S3 [2 of 3]

```
order 3   order 2
  1          1          1 copy

  1         -1          1 copy

 1  3      -1  0        2 copies
-1 -2       1  1
```

Can always conjugate regular rep. into integral irreducibles.

- Because the integers are a principle ideal domain, you can always change the basis by a transformation of determinant 1 to make it reduce (**not** decompose) into rational irreducibles written over the ordinary integers.
- That still leaves division rings and irrationalities to contend with!

To do this

- Start with any integral representation (e.g. the regular representation)
- Take any rational invariant subspace
- Take **all** the integral vectors in that space
- That is clearly invariant.
- You can complete that to an basis for the whole (integral) space you started with.
- You have now integrally reduced it.

C3 mod 3

Where are the 3 dimensions of the regular representation mod 3?

In the regular basis, $a + b.t + c.t^2$ gives

```
a  b  c
c  a  b
b  c  a
```

In a new basis we get, for example

```
1  1  0    1  2  2      x  y  z
0  1  1    0  1  2      0  x  y
0  0  1    0  0  1      0  0  x
```

Where x=a+b+c y=b+2c z=2c

Adding up the dimension of the group algebra – S3

- Mod all primes except 2 and 3, there are irreducibles of sizes 1, 1 and 2.
- $1^2 + 1^2 + 2^2 = 6$
- Mod 2, irreducibles 1 and 2, but there is an indecomposable

```
1  0      1  1
0  1      0  1
```

S3 mod 3

- Group algebra is 6 dimensional
- Decomposes as the direct sum of two distinct 3 dimensional indecomposables.

```
1  0  0    1  1  0
0 -1  0    0  1  1
0  0  1    0  0  1

1  -1  1.-1  -1.1  1.-1.1  -1.1.-1
```

“Cyclic” modules

- A representation is said to be cyclic if there is a vector such that its G-images span the whole space.
- A module is cyclic if and only if it is a quotient of the regular representation
- Hence we can see all the dimensions of the group algebra in cyclic modules.

Some groups

- An – alternating group on n points – the set of even permutations on n points.
- GLn(q) – the set of invertible n x n matrices over the field of q elements.
- Ln(q) is the determinant one matrices modulo scalars.

Example – A5 Char 0

	60	4	3	5	5
p power		A	A	A	A
p’ part		A	A	A	A
ind	1A	2A	3A	5A	5B
+	1	1	1	1	1
+	3	-1	0	-b5	*
+	3	-1	0	*	-b5
+	4	0	1	-1	-1
+	5	1	-1	0	0

Example – A5 mod 2

	60	3	5	5
p power		A	A	A
p’ part		A	A	A
ind	1A	3A	5A	5B
+	1	1	1	1
–	2	-1	*	b5
–	2	-1	b5	*
+	4	1	-1	-1

Example – A5 mod 3

	60	4	5	5
p power		A	A	A
p’ part		A	A	A
ind	1A	2A	5A	5B
+	1	1	1	1
+	3	-1	-b5	*
+	3	-1	*	-b5
+	4	0	-1	-1

Example – A5 mod 5

	60	4	3
p power		A	A
p’ part		A	A
ind	1A	2A	3A
+	1	1	1
+	3	-1	0
+	5	1	-1

A5 permutation module mod 5

- Clearly the space [x x x x x] is fixed by all permutations.
- The set [a b c d e] where a+b+c+d+e=0 (mod 5) is also an invariant subspace
- Because the degree is divisible by 5, this contains the [x x x x x] vectors

A5 mod 5

- One summand is 1.3.1 – permutation on 5
- Other summand is 3.(1+3).3
- 1x1 3x3 5x5 1x3 1x1 3x1 3x3 3x3
- 1 9 25 3 1 3 9 9 = 60

Last example L3(2)

- The set of all invertible 3x3 matrices with entries in F2.
- Order is 7.6.4=168
- For any matrix, easy to find centralizer so we can collect the six conjugacy classes.
- Permutation on vectors provides one character.
- Not too hard to get the rest.

Example – L3(2) Char 0

	168	8	3	4	7	7
p power		A	A	A	A	A
p' part		A	A	A	A	A
ind	1A	2A	3A	4A	7A	B**
+	1	1	1	1	1	1
o	3	-1	0	1	b7	**
o	3	-1	0	1	**	b7
+	6	2	0	0	-1	-1
+	7	-1	1	-1	0	0
+	8	0	-1	0	1	1

Example – L3(2) mod 2

	168	3	7	7
p power		A	A	A
p' part		A	A	A
ind	1A	3A	7A	B**
+	1	1	1	1
o	3	0	b7	**
o	3	0	**	b7
+	8	-1	1	1

Example – L3(2) mod 3

	168	8	4	7	7
p power		A	A	A	A
p' part		A	A	A	A
ind	1A	2A	4A	7A	B**
+	1	1	1	1	1
o	3	-1	1	b7	**
o	3	-1	1	**	b7
+	6	2	0	-1	-1
+	7	-1	-1	0	0

Example – L3(2) = L2(7) mod 7

	168	8	3	4
p power		A	A	A
p' part		A	A	A
ind	1A	2A	3A	4A
+	1	1	1	1
+	3	-1	0	1
+	5	1	-1	-1
+	7	-1	1	-1

L2(p) mod p

- 2 x 2 matrices mod p, determinant 1

$\begin{matrix} -1 & 0 \\ 0 & -1 \end{matrix}$ is in the centre, so we can factor it out to get L2(p) – simple for p≥5

Action on the space of homogenous polynomials of degree 2.d in two variables is a representation of dimension 2.d + 1.

Representations – Theory and Practice – Lecture 12

Blocks

Blocks of defect zero

Decomposing permutation representations

Decomposing the regular representation

Overview

- For a group and a prime, there is a small set of "blocks"
- Every ordinary irreducible belongs to a block
- Every modular irreducible belongs to a block
- ***Everything interesting happens mod p within a block.***

Defect groups

- Every block has a well-defined (up to conjugacy) p-group called the Defect Group of the block.
- This group is the Sylow-p subgroup of the centralizer of at least one p' element.
- The representation theory of the defect group has great influence on the block.

Blocks - preamble

- Adding up any conjugacy class in any representations gives a matrix that commutes.
- The eigenvalues of it decompose the representation
- So for each indecomposable representation mod p and each conjugacy class there is a well-defined eigenvalue which must be the same for all constituents.
- (otherwise it would decompose!)

Blocks - definition

- Hence an early question is to ask, for each modular irreducible, what eigenvalue you get for each class.
- This gives an equivalence relation on the irreducibles – do they give the same eigenvalue on all classes
- The equivalence classes are the blocks.
- An indecomposable must have all its constituents from the same block

Idea behind blocks from ordinary character table

- But every modular irreducible is a constituent of the regular representation mod p
- Which is the reduction mod p of the integral regular representation
- Where the eigenvalues of the class sums can be computed from the character table

Ordinary characters in p blocks

- The possible eigenvalues can be worked out from the ordinary character table as character value times class size divided by the degree.
- Hence the ordinary characters come in blocks mod p also

Example – A5

	60	4	3	5	5
p power		A	A	A	A
p' part		A	A	A	A
ind	1A	2A	3A	5A	5B
+	1	1	1	1	1
+	3	-1	0	-b5	*
+	3	-1	0	*	-b5
+	4	0	1	-1	-1
+	5	1	-1	0	0

P-blocks of A5

1A	**2A**	**3A**	**5A**	**5B**	**2**	**3**	**5**
1	15	20	12	12	A	C	F
1	-5	0	4b5	*	A	D	F
1	-5	0	*	4b5	A	E	F
1	0	5	-5	-5	B	C	F
1	3	-4	0	0	A	C	G

Defect zero representations

- Define an ordinary irreducible to be "defect zero mod p" if its degree is divisible by the order of the Sylow-p subgroup. (We will generalize this later).
- It is alone it its p-block,
- Is irreducible mod p
- so is a direct summand of any representation that contains it as a constituent.

Defect zero alone in block

- Σ H(c).χ_1(c).χ_2(c)*) is group-order for $\chi_1=\chi_2$ and zero otherwise
- If the Sylow-p subgroup has order S, then (Σ H(c).χ_1(c).χ_2(c)*)/S is non-zero mod p iff $\chi_1=\chi_2$
- (Σ H(c).χ_1(c).χ_2(c)*)/deg (χ_1) is nonzero iff $\chi_1=\chi_2$ and deg (χ_1) is divisible by S
- So if we take χ_2 as a defect zero character, $\chi_1=\chi_2$ is the only character with (Σ H(c).χ_1(c).χ_2(c)*)/deg (χ_1) non-zero mod p
- Hence $\chi_1=\chi_2$ is alone in its block

Irreducible mod p

- Suppose otherwise. Take a field in which it can be written, and take the local domain (denominators not in a maximal ideal π)
- Reduction mod π is now defined.
- Suppose there was an invariant subspace mod π. Take a vector v in it with $x \neq 0$ mod π in the i-th coordinate.
- Make M as the matrix whose i-th row is any lift of v, and add up all conjugates of M
- This has trace x/Z (Z the group order divided by degree) so is a scalar not 0 mod π. Hence the images of v span the space – so v wasn't in an invariant subspace after all.

Far too many indecomposables

- But we can take any finite set of representations and look at the direct summands of them
- If we take the set of all permutation representations . . .
- The summands all lift to characteristic zero!
- And in particular the summands of the regular representation are important.

Trivial source modules

- A representation is said to have trivial source if it is isomorphic to a direct summand of a permutation module
- It (Hensel) lifts to characteristic zero
- So do all Homs between them
- . . . So DimHom (A,B) is the ordinary character inner product between the lifts of A and B.

Example

- 4 dimensional representation mod 3 of A5
- Permutation on 5 points is 1 + 4 direct sum
- (since 5 is coprime to 3)
- 4 is irreducible mod 3 and trivial source
- Permutation action of A5 on 6 points
- (As ordinaries 1, 5)
- DimHom is 0 so the modular 4, although a constituent, is neither a sub nor a quotient.

Lemma. Transitive permutations fix only one vector

- Independent of the field . . .
- A transitive permutation representation fixes only the point [x x x x . . .]
- For if it fixes [x a b c . . .] then a=x since there is a permutation taking the first point there, as it is transitive.
- So the map from fixed points in characteristic zero to characteristic p is onto.

So Homs between permutation modules lift to characteristic 0

- A Hom from one transitive permutation module A to another B is specified by giving where one point goes
- And this works if and only if it goes to a vector fixed in B by A's point stabilizer
- But this lifts to characteristic zero
- So the Hom lifts also

Endomorphisms of permutation modules

- This applies in particular to hom(A,A) – the endomorphism ring of A.
- Every endomorphism of a permutation module lifts.

Idempotents lift [Hensel]

- Suppose e_1=e is the idempotent mod p
- Define x as any lift of e_i mod p^{i+1}
- So $(x^2 - x)^2 = 0$ mod p^{i+1}
- Define $e_{i+1} = 3x^2 - 2x^3$
- This is $3e_i - 2e_i = e_i$ mod p^i
- Notice that $3.x^2–2.x^3 = x^2$. something
- And $3.x^2–2.x^3–1 = (x - 1)^2(-2x-1)$
- So $(e_{i+1})^2–(e_{i+1}) = e_{i+1}.(e_{i+1}–1)$
- $= [3.x^2–2.x^3] [3.x^2–2.x^3–1]$
- is divisible by the square of x(x-1) which is zero

Decompositions of permutation modules lift to characteristic 0.

- Decompositions are given by the idempotents of the endomorphism ring
- Which lift to characteristic zero.
- Hence every direct summand mod p of a permutation module is the reduction mod p of an ordinary (p-adic) representation.
- Notice that this applies to the regular representation also.

Putting all this together

- Any mod-p direct summand of a permutation module lifts to characteristic zero (an ordinary representation)
- and homs between them lift also (so the dimension can be computed using ordinary character theory)

Matrices commuting with the regular representation.

- **Q.** What commutes with the right-regular representation $x_s.g = x_{sg}$?
- **A.** The left-regular representation $x_s.h = x_{hs}$
- The actions obviously commute – both taking x_s to x_{hsg} since a group is associative
- But the dimension is correct – if you know where an endomorphism takes x_1 you know where it takes $x_s = x_1.s$.

Remark

- The ring on endomorphisms of the regular representation is isomorphic to that regular representation!
- Hence (from Frobenius-Schur) we know what orthogonal idempotents look like (just a 1 on the diagonal of some irreducible)
- Hence we know how the regular representation ***decomposes***.

Idempotents of the group algebra

- Let e be an element of the group algebra that is 1 at the top left of some irreducible and zero elsewhere.
- This may not be idempotent, but some power of it will be (look at the Jordan Blocks)

Regular representation decomposition.

- Suppose the irreducible representations are ρ_i of degrees d_i
- Then the regular representation decomposes as d_i copies of a module π_i corresponding to ρ_i.
- We call π_i the principle indecomposable module for ρ_i, or PIM.
- Also called projective indecomposable.

Properties of the PIM

- The PIM π_i has a unique top composition factor, isomorphic to ρ_i … $\pi_i \rightarrow \rho_i$
- The PIM is projective – take any module homomorphism $M \rightarrow \rho_i$ then there is a map from π_i to M with $\pi_i \rightarrow M \rightarrow \rho_i$

Representations – Theory and Practice – Lecture 13

Decomposition of the regular representation.

Introduction to vertices and sources.

Story so far

- Direct sum decompositions of permutation representations in characteristic p lift to the p-adics.
- Class sum eigenvalues define blocks.

Apology

- I am very familiar with the results in today's lecture, but am shaky on the proofs – it is many years since I did this stuff, and have forgotten lots.
- In the meantime I have developed my own way of thinking about these things, and find that my approach differs significantly from the literature.
- I therefore have no way of continue to provide proofs of all the results.

Little diversion - G-opp

- Let G be a group.
- Define a new group G-opp by using the same set, but defining a*b as ba.

- G-opp is isomorphic to G
- Map g to g^{-1}
- And notice that $(xy)^{-1} = y^{-1}x^{-1}$

Decomposing the regular representation.

- We now wish to investigate the decomposition of the regular representation. It would be nice if we knew the structure of the endomorphism ring . . .
- But that would be too much to ask.
- What we find is that the endomorphism ring is ***isomorphic to the regular representation itself***

Matrices commuting with the regular representation.

- **Q.** What commutes with the right-regular representation $x_s.g = x_{sg}$?
- **A.** The left-regular representation $x_s.h = x_{hs}$
- The actions obviously commute – both taking x_s to x_{hsg} since a group is associative
- But the dimension is correct – if you know where an endomorphism takes x_1 you know where it takes $x_s = x_1.s$.

Group ring approach

- We may define an algebra – the group ring – by taking a basis indexed by the group elements and taking $x_a.x_b = x_{ab}$.
- In my opinion this does not sit well with other parts of the theory, and tensor products in particular, but I seem to be in a minority of 1.
- The literature therefore does not distinguish sums elements of the group and endomorphisms of the regular representation.
- I have not been able in the time available to convert the book proofs into my language.

What happens?

- Each modular irreducible has a corresponding PIM (principle or projective indecomposable module)
- There is a decomposition matrix D that can be read two ways.
  - Rows indexed by the ordinary irreducibles
  - Columns indexed by the modular irreducibles
- How the ordinary breaks up as modulars
- How the PIM breaks up as ordinaries

Decomposition matrix - A5 mod 2

	1	**2**	**2'**	**4**
1 -	1	0	0	0
3 -	1	1	0	0
3' -	1	0	1	0
4 -	0	0	0	1
5 -	1	1	1	0

So ordinary 3 = 1+2

PIM for 1 = 1+3+3+5

Why does this happen?

- Idempotents of endomorphism ring . . .
- ***are*** idempotents of the group algebra
- Obtained for example by taking a 1 in the top left of an irreducible and zero everywhere else (including on the other modular irreducibles).
- The number of copies is the number of different places along the diagonal – the degree of the irreducible.

Hand-waving explanation

- The PIM is e.R.e
- So if there were a hom onto any other modular irreducible
- It would be e.R.e -> something, but e is zero on the other irreducibles and rank 1 on the one we started with
- So we know where it takes a basis vector of the regular representation and hence where it takes everything else.

Structure of a PIM

- It has a unique copy of "its" irreducible on the top – it cannot have a hom onto anything else, and it only has one hom onto the starting one.
- Using duality (transpose-inverse = **) we can show that the ** PIM has the ** irreducible on the top, so the PIM has the ***same*** irreducible as the unique irreducible submodule.

PIM is Projective

- Suppose we have any module with a particular irreducible as a constituent.
- So we have a hom from a submodule to the irreducible
- We may first take the smallest submodule with that hom. It has the irreducible as the unique top composition factor.
- Now take any vector not in the kernel and we have a map from the regular representation to our submodule

PIM is projective - 2

- The regular representation is the direct sum of the PIMs, so there must be some summand that maps to the module.
- Hence the PIM is the largest module with the irreducible as a top composition factor, and all such modules are quotients of the PIM.

Read D-matrix two ways.

- Take this idempotent. Start with an ordinary representation. Reduce it mod p and the rank of this tells you two things. . .
- how often that modular is in the ordinary.
- the dimension of the space of vectors in its image, hence the number of times the ordinary occurs in the PIM (which is a direct summand of a permutation!)

Introduction to Vertices and Sources

- In ordinary character theory, one can prove ***Frobenius reciprocity*** using character formulae.
- If ρ is a representation of G and
- σ is a representation of a subgroup H
- $\langle \sigma\uparrow, \rho \rangle = \langle \sigma, \rho\downarrow \rangle$
- The number of times ρ is a summand of σ induced equals the number of times σ appears in the restriction of ρ.

Works a bit for coprime index

- If you restrict to a subgroup of index coprime to the characteristic, there is a summand that you can induce up which has the original module as a summand.
- In particular if you restrict to the Sylow-p subgroup, some summand of that induces up to give your original module as a summand.

Won't be proving this – not today, anyway

- The proof is not that hard, but I tried to put it in and found it hard to get straight.
- The ideas are similar to what happens if it is the trivial representation of H that you induce up.
- You can average idempotents and take obvious submodules . . .

Green's work

- By investigating this, J. A. Green was able to show that every indecomposable has a "Green correspondent" which consists of some well-defined (up to conjugation) representation of the normalizer of some p-group.

Module and Green Correspondent

- The p-group is called the Vertex
- The Green correspondent restricted to the vertex is the source.
- The module is a summand of the induced Green correspondent.
- If the module is a summand of an induced module, the module induced from has the "same" vertex and source,

Green's theorem

- Induce an ***absolutely indecomposable*** representation from a ***normal*** subgroup of index p (the characteristic) and the result is absolutely indecomposable.
- I won't be proving this either. It is surprisingly hard.

Representations – Theory and Practice – Lecture 14

Computing the modular characters
- an example
- A7 mod 5.

Some comments on indicators.

Computing modular characters

- In the case of A7 mod 5, the Sylow 5 subgroup is cyclic, so we could use the methods of cyclic defect and Brauer trees.
- I have not used that, partly because I have not covered it yet
- And partly because I wish to demonstrate the general techniques.
- There is no algorithm for computing the modular characters, and often it gets too difficult to do theoretically and we must resort to a computer to handle the matrices explicitly.

Example – A7 mod 5

2520	24	36	9	4	5	12	7	7
p power	A	A	A	A	A	AA	A	A
p' part	A	A	A	A	A	AA	A	A
ind	1A	2A	3A	3B	4A	5A	6A	7A	B**
+	1	1	1	1	1	1	1	1	1
+	6	2	3	0	0	1	−1	−1	−1
o	10	−2	1	1	0	0	1	b7	**
o	10	−2	1	1	0	0	1	**	b7
+	14	2	2	−1	0	−1	2	0	0
+	14	2	−1	2	0	−1	−1	0	0
+	15	−1	3	0	−1	0	−1	1	1
+	21	1	−3	0	−1	1	1	0	0
+	35	−1	−1	−1	1	0	−1	0	0

Example – A7 mod 5

2520	24	36	9	4	5	12	7	7
p power	A	A	A	A	A	AA	A	A
p' part	A	A	A	A	A	AA	A	A
ind	1A	2A	3A	3B	4A	5A	6A	7A	B**
+	1	1	1	1	1	1	1	1	1
+	6	2	3	0	0	1	−1	−1	−1
o	10	−2	1	1	0	0	1	b7	**
o	10	−2	1	1	0	0	1	**	b7
+	14	2	2	−1	0	−1	2	0	0
+	14	2	−1	2	0	−1	−1	0	0
+	15	−1	3	0	−1	0	−1	1	1
+	21	1	−3	0	−1	1	1	0	0
+	35	−1	−1	−1	1	0	−1	0	0

First step – blocks mod 5. 10, 10, 15 and 35 all defect zero so irreducible mod 5. Remainder is all in one block - the principle block – 1, 6, 14a, 14b, 21.

Can remove the 5-singular columns to get a first working list of "genuine" Brauer characters of principle block.

Example – A7 mod 5

2520	24	36	9	4	12	7	7
p power	A	A	A	A	AA	A	A
p' part	A	A	A	A	AA	A	A
ind	1A	2A	3A	3B	4A	6A	7A	B**
+	1	1	1	1	1	1	1	1
+	6	2	3	0	0	−1	−1	−1
+	14	2	2	−1	0	2	0	0
+	14	2	−1	2	0	−1	0	0
+	21	1	−3	0	−1	1	0	0

A7 contains L2(7) (order 168) as a subgroup. 5 does not divide the order of L2(7) so its 5-modular characters are just the ordinary characters. The 6 dimensional representation is irreducible restricted to L2(7) so irreducible for A7.

L32(7) Characterisic 0

	168	8	3	4	7	7
p power		A	A	A	A	A
p' part		A	A	A	A	A
ind	1A	2A	3A	4A	7A	B**
+	1	1	1	1	1	1
o	3	-1	0	1	b7	**
o	3	-1	0	1	**	b7
+	6	2	0	0	-1	-1
+	7	-1	1	-1	0	0
+	8	0	-1	0	1	1

Example – A7 mod 5

	2520	24	36	9	4	12	7	7
p power		A	A	A	A	AA	A	A
p' part		A	A	A	A	AA	A	A
ind	1A	2A	3A	3B	4A	6A	7A	B**
+	1	1	1	1	1	1	1	1
+	6	2	3	0	0	-1	-1	-1
+	14	2	2	-1	0	2	0	0
+	14	2	-1	2	0	-1	0	0
+	21	1	-3	0	-1	1	0	0

Also the permutation representation on L2(7) is on 15 points. It is actually 1+14b since it is 3B that is in L2(7), not 3A (by restriction of 6).

Hence there is another trivial constituent (since 5 divides 15) in 14b, leaving a 13-dimensional representation.

Example – A7 mod 5

	2520	24	36	9	4	12	7	7
p power		A	A	A	A	AA	A	A
p' part		A	A	A	A	AA	A	A
ind	1A	2A	3A	3B	4A	6A	7A	B**
+	1	1	1	1	1	1	1	1
+	6	2	3	0	0	-1	-1	-1
+	14	2	2	-1	0	2	0	0
+	13	1	-2	1	-1	-2	-1	-1
+	21	1	-3	0	-1	1	0	0

6+21=13+14 on 5-regular classes.

There is an (irreducible) 6 in 13+14. Can't be in 13 since subtracting the 6 character from 13 we get degree 7 value -5 on 3A, which is impossible (contains the trivial character of cyclic 3 with multiplicity -1) Hence 6 is in 14a

Example – A7 mod 5

	2520	24	36	9	4	12	7	7
p power		A	A	A	A	AA	A	A
p' part		A	A	A	A	AA	A	A
ind	1A	2A	3A	3B	4A	6A	7A	B**
+	1	1	1	1	1	1	1	1
+	6	2	3	0	0	-1	-1	-1
+	8	0	-1	-1	0	3	1	1
+	13	1	-2	1	-1	-2	-1	-1
+	21	1	-3	0	-1	1	0	0

Now 21 really is 8 + 13 and we can discard it.

The 8 is irreducible restricted to L2(7) so is irreducible.

Example – A7 mod 5

	2520	24	36	9	4	12	7	7
p power		A	A	A	A	AA	A	A
p' part		A	A	A	A	AA	A	A
ind	1A	2A	3A	3B	4A	6A	7A	B**
+	1	1	1	1	1	1	1	1
+	6	2	3	0	0	-1	-1	-1
+	8	0	-1	-1	0	3	1	1
+	13	1	-2	1	-1	-2	-1	-1

The 13 is 6+7 restricted to L2(7). Since there is only one more irreducible to find, either the 13 is irreducible, or it is 6+7 for the 6 shown above. But restricted to <3A> 13 has 3 trivial characters and the 6 has 4. Hence the 13 is irreducible and the characters above are all correct. Sorting, and putting the defect zero characters back, we get . . .

Example – A7 mod 5

	2520	24	36	9	4	12	7	7
p power		A	A	A	A	AA	A	A
p' part		A	A	A	A	AA	A	A
ind	1A	2A	3A	3B	4A	6A	7A	B**
+	1	1	1	1	1	1	1	1
+	6	2	3	0	0	-1	-1	-1
+	8	0	-1	-1	0	3	1	1
o	10	-2	1	1	0	1	b7	**
o	10	-2	1	1	0	1	**	b7
+	13	1	-2	1	-1	-2	-1	-1
+	15	-1	3	0	-1	-1	1	1
+	35	-1	-1	-1	1	-1	0	0

Projective indecomposables

- Four (10,10,15,35) of defect zero

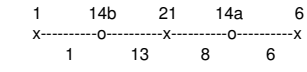
Decomposition matrix for principle block is

	1	**6**	**8**	**13**
1	1	0	0	0
6	0	1	0	0
14a	0	1	1	0
14b	1	0	0	1
21	0	0	1	1

Hence PIM constituents are (1,1,13) (6,6,8) (6,8,8,13) and (1,8,13,13)

Self-dual with unique top and unique bottom, the module structure is uniquely determined in each case.

Brauer Tree of A7



PIM structures

1.13.1 13.(1+8).13 8.(13+6).8 6.8.6

14 of the 16 non-projective indecomposables are subs or quotients of projectives. The other two are (1+8).(13+6) and (13+6).(1+8)

The four irreducibles 1 13 8 6 are indecomposable.

Six with two constituents 1.13 13.1 13.8 8.13 8.6 6.8

Four with three constituents 13.(1+8) (1+8).13 8.(13+6) (13+6).8

Indecomposables of A7 mod 5

- Since the Sylow subgroup is cyclic, it is possible in this case to find all indecomposable representations.
- I propose to sketch this.
- Those whose vertex is trivial are projective indecomposables already found.
- The remainder have vertex cyclic-5 and have a Green correspondent which is an indecomposable of the normalizer 5.4
- We therefore need to understand the indecomposable representations of 5.4

Investigating the Sylow-5 normalizer.

- Is a group of order 20 – 5.4. We may give it concretely as $x^5=y^4=1$; $y^{-1}xy=x^2$.
- Besides the regular representation, a group of order 5 has four indecomposables – dimension 1,2,3 and 4 (Jordan blocks)
- Cyclic 4 has four irreducibles mod 5, where x is represented by [1], [2], [3] or [4] (mod 5).
- Hence 5.4 has 16 non-projective indecomposables which we may name as F(a,b) where a is the dimension of the indecomposable (1,2,3 or 4) and b is the number mod 5 that y is represented by in the bottom constituent.

F(3,2)

An example indecomposable of 5.4

$$x = \begin{pmatrix} 1 & 4 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad y = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Green Correspondents

```
F(1,1)  1  1
F(1,4)  6  6
F(1,2) 21  13.8
F(1,3) 21  8.13
F(2,2) 22  13.(1+8)
F(2,4) 22  (1+8).13
F(2,3) 27  8.(13+6)
F(2,1) 27  (13+6).8
F(3,3) 8   8
F(3,2) 13  13
F(3,1) 28  (1+8).(13+6)
F(3,4) 28  (13+6).(1+8)
F(4,1) 14  1.13
F(4,2) 14  13.1
F(4,3) 14  8.6
F(4,4) 14  6.8
```

Demonstration of Green correspondents.

- Trivial character is clearly F(1,1)
- So degree 6 must be F(1,4) since its dimension is 1 mod 5 and it is self-dual.
- The 13 is the projective (permutation on 15) with 1 removed top and bottom so is F(3,2).
- Hence the 8 must be the other self-dual dimension 3, namely F(3,3)
- Now dimension, the bottom constituents and duality gives the rest.

Indicators

- In odd characteristic, if a self-dual modular occurs with odd multiplicity in a self-dual ordinary, they have the same indicator.
- This gives all the indicators in this case.
- (and in all cases, according to Thompson)

Which quadratic form?

- If the degree is even and the indicator is +, there are precisely two quadratic forms and one of them is fixed and the other isn't.
- The published modular character tables do not indicate which one is fixed.
- Indeed this is true even for the ordinary atlas. For example the 6 dimensional representation of A7 is of "plus" type over a field, I believe, precisely when –7 is a square. I did campaign that this "–7" be included in the Atlas, but lost.

Other information not given in Atlas character tables.

- If the indicator is "+", it is not stated whether the representation is writable in the field. In fact it almost always is writable. W. Feit has a paper on the subject and lists the exceptions (about seven, I think).
- If the indicator is "–", it is not stated whether the representation can be written over a quadratic extension (which I believe is in fact always the case). Again, see Feit.
- etc. etc.

Tensoring Jordan Blocks

Suppose we tensor the 3-dimensional indecomposable for cyclic-5 with the 2 dimensional one.

How does that decompose?

Answer 1+5

We will investigate this more next time.

Representations – Theory and Practice – Lecture 15

Revise Jordan Blocks

Modular representations of cyclic groups

Species

Jordan block decomposition.

- Every matrix is conjugate (uniquely) to the direct sum of Jordan Blocks if you extend the field enough to contain the eigenvalues

λ 1 0 0 0 0 [To prove this, first decompose
0 λ 1 0 0 0 into the different eigenspaces, then
0 0 λ 1 0 0 subtract λ.I to get a nilpotent matrix.
0 0 0 λ 1 0 Now conjugate the nilpotent matrix
0 0 0 0 λ 1 so that it looks like a Jordan Block]
0 0 0 0 0 λ

Which Jordan blocks have order p where p is the characteristic?

- λ must be 1
- and the size must be at most p

Mod 3 indecomposables

- Hence we can show that every representation of a cyclic group of order 3, in characteristic 3, is the direct sum of the three indecomposables

```
1  1  0     1  1        1
0  1  1     0  1
0  0  1
```

What about dihedral 6

- There are six indecomposables.
- First take the three indecomposables of C3.

1 2 0	1 1 0	1 0 0	2 0 0
0 1 1	0 1 2	0 2 0	0 1 0
0 0 1	0 0 1	0 0 1	0 0 2
A	A^2	B_1	B_2

$\langle A,B_1 \rangle$ and $\langle A,B_2 \rangle$ are both representations of the dihedral group of order 6.

What information might we ask about a representation

- The Jordan Block structure of all its elements seems like a natural one.
- In characteristic zero, this is done by characters.
- Characters are linear maps S from representations to the complex numbers with $S(\rho + \sigma) = S(\rho) + S(\sigma)$
- Which linear maps on Jordan Blocks shall we choose?

Tensor products

- Another property of characters that we might like is that the tensor product property $S(\rho \times \sigma) = S(\rho) \times S(\sigma)$
- Maps with these properties are called species – columns of character tables are examples of species but there are many many more.

Species of a group

- A species is a non-zero map from the set of representations of a group to the complex numbers such that
- [direct sum] $S(\rho + \sigma) = S(\rho) + S(\sigma)$
- [tensor product] $S(\rho \times \sigma) = S(\rho) \times S(\sigma)$
- A bit like a column of the character table
- The zero map has these properties but we do not consider that to be a species.

Species by restriction

- If S is a species of a subgroup H of G, a species of G is readily obtained by restricting to H and then using the species you have.
- It turns out that the species obtained by restriction to cyclic groups gives precisely the Jordan Block decomposition.
- This is because there are precisely n species of a cyclic group of order n

Example – cyclic 2 mod 2

- There are only two indecomposables – dimension 1 and 2.
- 1x1=1 1x2=2 2x2=2+2
- Any species has value y on the trivial representation where y.y=y. Hence y=0 or y=1. But y=0 implies the species is everywhere zero ($1 \times \rho = \rho$) and we just ignore this "species"
- Hence all species have value 1 on the trivial representation.

Species of cyclic 2 mod 2.

- 2 x 2 = 2 + 2, so if the species has value z on the 2, we have that z x z = z+z whence z=2 or z=0.
- Hence we get a complete species table

1 1
2 0

In this case two representations with the same value on all species are isomorphic.

Although true for cyclic groups, this is not true for groups in general, though a counterexample has only been found fairly recently.

Cyclic 3

- The first difficulty is to determine what the Jordan Block decomposition of the tensor square of the 2.
- In other words, decompose

1 1 1 1 Rank of Z-1 is 2
0 1 0 1 Rank of $(Z-1)^2$ is 1
0 0 1 1 Hence it must be 3 + 1
0 0 0 1

3 x 2 = 3+3; 3x3 = 3+3+3

- These can be computed in a similar way
- Or you can notice that you can take the 3 as permuting the basis vectors, so permuting the columns in the tensor product, so any basis for the first column gives a direct sum decomposition into 3s.
- Suppose a species has value x on the 3 and y on the 2. Then x.y=2.x and y.y=1+x.
- From the first, x=0 or y=2. From the second, if x=0 then y=1 or y=-1, if y=2 then x=3.

Cyclic 3

- Hence the full list of species is

  1 1 1
  2 1 -1
  3 0 0

Nothing very obvious!

The second column says that the number of non-3 Jordan Blocks is a species.

Cyclic 5 is an irrational mess

- Let x, y, z be species values on 2, 3, 4 respectively. Then we have . . .
- x.x=1+y
- x.y=x+z $x^3=2x+z$
- x.z=y $x^4=2+3y = 3x^2-1$
- $x^4-3x^2+1 = 0$
- Roots are b5, -b5 and their algebraic conjugates.

Species of cyclic 5

- 1 1 1 1 1
  2 b5 * -b5 *
  3 * -b5 * -b5
  4 1 1 -1 -1
  5 0 0 0 0

The only rational column is the degree.

What do the irrationalities mean?

- I believe it is true that if you take an ordinary representation with an element of order 5 that is ***rational*** – conjugate to all its powers that have order 5 – then reduction modulo 5 cannot give Jordan Blocks of sizes 2 or 3.
- But I don't really know.

Cyclic group order p in characteristic p

- Take L2(complexes) - 2x2 matrices of determinant 1
- And take an element of order 2.p in this.
- The character of this element and its odd powers on the representations of degree 1, 2, . . . p satisfy the "tensor product conditions" for the species of a cyclic group of order p. Making this precise is a bit messy.
- So there are p of them – the same as the number of indecomposables.

Brauer Species

- A species that is obtained by restricting to a p' subgroup is just a column of the Brauer character table
- They determine the constituents, as previously discussed.
- They can all be obtained by restricting to cyclic p' subgroups.

Jordan Block equivalence?

- Two representations with the same Jordan Block structure for every element are clearly a bit more similar than just having the same constituents.
- I am not aware of anyone every looking at this equivalence relation.

More generally

- All species can be obtained by restricting to normalizers of p-groups by p' elements.
- I'm afraid these groups are called the **origin of the species**!
- The pun was intended.

Species do not characterize.

- I forget the author [sorry] but it has been proved that there are two non-isomorphic representations of 2 x 2 x 2 with the same value on ***every*** species.
- Hence species do not, in general, characterize the representation up to isomorphism.
- But species do give a huge amount of information about the representations.

Elements of order 2.

- In the case of an element t of order 2, there is another species trick available – the "middle".
- The kernel of 1+t modulo its image is a representation of (X) the centralizer of t modulo t.
- $M(\rho) \times M(\sigma) = M(\rho \times \sigma)$
- So any species of X is a species of the whole group!

Middle

- A.B.A x C.D.C is
- **AC.(AD+BC).(AC**+BD+*AC).(AD+BC).AC*
- But the involution adds the bold spaces into the italic ones, so only the BD is in the kernel modulo the image.
- This only works for elements of order 2 in characteristic 2!

What about Cyclic-3

- The 1 1 0 column gives us hope that there might be a middle for these elements also.
- B is the action on the 2s and C on the 1s
- Then the new B is $B_1.B_2$. $C_1.C_2$
- And the new C is $B_1.C_2+B_2xC_1$
- So the **constituents** work but the module structure somehow doesn't
- Again, more work is needed here.

Cyclic 5 and greater

- Since all the columns of the species table except the degree are irrational
- There is no hope of defining a middle module here.

Representations – Theory and Practice – Lecture 16

Defect groups of representations and conjugacy classes

Brauer Correspondence and Brauer's main theorems.

Blocks

- The eigenspaces of the class sums, reduced mod p, decompose any modular representation into summands from the various blocks.
- Hence when studying representations in characteristic p it is natural to study them one block at a time.

Centre of group algebra mod p

- Decomposition into blocks comes from eigenvalues of class sums
- So we turn our attention to how the mod-p centre of the group algebra works.
- In particular when the product of two classes contains a third class with multiplicity $x \neq 0 \pmod{p}$ times.

Everything "up to conjugacy"

- The remainder of this lecture would be entirely cluttered with the words "conjugate to" if I left them in wherever necessary.
- I have therefore omitted this wholesale.
- Please understand that often an element or subgroup "is" another often means "is conjugate to".
- And G contains H means some conjugate of G contains some conjugate of H.

Defect groups of conjugacy classes.

- Given a conjugacy class A of elements of a group
- The Sylow-p subgroup of its centralizer is its defect group D(A).
- It is defined up to conjugacy.

Combinatorial lemma

- The product of two class sums A.B contains a third class sum C zero (mod p) times unless possibly D(A) and D(B) both contain D(C).
- So mapping classes to their defect group, *multiplying classes can only make the defect group smaller*.

Proof of Combinatorial Lemma

- Let D be the Sylow-p subgroup of the centralizer of an element z
- Let A and B be any two conjugacy classes (of G) and consider those with a.b=z.
- D centralizes z
- So the (conjugacy) orbits of D on pairs (a,b) are of size some multiple of p unless D actually centralizes both a and b.

A block B

- Has a "defect group" associated with it.
- This is a p-group.
- It contains the vertex of any representation in the block.
- It is the Sylow subgroup of the centralizer of some p' element in the group.

Definition

- The defect group of a block is the smallest Sylow-p subgroup of the centralizer of an element with non-zero eigenvalue.

Proof that defect groups exist.

- Consider the set of conjugacy classes with non-zero value on a central character.
- If I multiply two such, the result is the sum of classes, and there must be at least one occurring with non-zero multiplicity (mod p) that also has non-zero value.
- But this can only make the Defect Group smaller. . .
- Now multiply any class X by one with the smallest defect group and the result, must contain one that is smallest, and therefore so does X.

A little terminology

- If the defect group has order p^d, we say that the block has defect d.
- In particular, if the defect group is trivial, the block has defect zero.
- The trivial character always has the full Sylow-p subgroup as its defect group, for the central product is zero unless the class size is coprime to p.
- This block is called the principle block.

Defect group contains the vertex.

- Given any indecomposable representation that lies in a block with defect group D,
- Then D contains a vertex for that representation
- In other words, the original indecomposable is a direct summand of some representation of D induced up to G.

Brauer's work.

- He was primarily interested in what modular characters can tell you about the ordinary character table.
- This work has been of critical importance in the classification of finite simple groups.
- I propose to sketch his work to the best of my ability - most of it without proof.

Brauer's main theorems

1. There is a bijection between blocks of G with defect group D and blocks of $N_G(D)$ with defect group D
2. Ordinary character values on elements with p part z respect (some of) the block structure of $C_G(z)$
3. The Brauer Correspondence takes principle blocks to principle blocks.

Brauer's first main theorem

- Is about blocks of G with defect group D and blocks of subgroups H of G containing both D and $C_G(D)$ also with defect group D
- Trouble is that things that are conjugate in G may no longer be conjugate in H
- So although the Brauer Correspondence still works
- It is quite hard in general to say what the map is ***from***

One statement of the 1st main theorem.

- Q When is D a defect group of a block of G?
- A When $N = N_G(D)/D$ has a block of defect zero.
- Indeed there is a bijection (the "Brauer correspondence") between the blocks of G and N with defect group D

How many blocks of defect zero does a group have?

- If G has a normal p-subgroup – none.
- But the simple group M_{24} has no defect zero block for p=2.
- So a p-group being a maximal normal subgroup of its normalizer is necessary, but not sufficient.

Brauer correspondence

- Given a p-group P, its “Brauerlizer” (my word) Br(P) is the group generated by it and its centralizer. Both it and its centralizer are normal in Br(P).
- There is an onto map from the blocks of Br(P) with defect group P and those of G with defect group P.

How does this map arise?

- It arises because, for each p-group P there is a homomorphism (the Brauer homomorphism) from the mod-p centre of the group ring of G to that of the centralizer of P
- The same old combinatorial lemma again.

Brauer Homomorphism

- Let G be a group, P a p-subgroup of G.
- Take the mod p class sums of both G and $C_G(P)$.
- Mapping each class sum of G to the sum of those elements that lie in $C_G(P)$ is a homomorphism.

Proof of Brauer Homomorphism

- Let A and B be two conjugacy class sums, and let A = **a** + *a* and B = **b** + *b* where the bold font represents those elements in $C_G(P)$ and italic those that do not.
- A.B= (**a** + *a*)(**b** + *b*)= **a b** + **a** *b* + *a* **b** + *a b*
- Clearly **a** *b* and *a* **b** have no elements in $C_G(P)$.
- And if z = *a b* then P cannot centralize *a* so the orbits of P all have size greater than 1 so zero mod p.

Sketch of Brauer correspondence

- Suppose we have a block b of $C_G(P)$
- Then by the Brauer Homomorphism we get a map from the mod-p centre of the G group algebra to that of $C_G(P)$.
- So we get a central character for G.
- In fact, (by inducing up a character from b) we can show that we get a single block of G. We call this b^G.

“Higher decomposition numbers”

- If we take an element x of order p^n and an ordinary irreducible character, we can restrict the character to x and split up into eigenspaces to get, for each eigenvalue (a root of 1) a representation of $C_G(x)/\langle x \rangle$
- We take the generalized modular representation obtained by summing these representations times their eigenvalue.

Brauer's second main theorem

- The characters with non-zero coefficients in a higher decomposition of an ordinary character all come from blocks of the centralizer of x whose defect group is the defect group of the original ordinary character.
- In particular the defect group is contained in that centralizer.

Combining these . . .

- This consists of just looking in the ordinary character table at the character values on the elements whose p-part is x.

Combining these . . .

- Brauer's second main theorem.
- This generalized modular character comes from blocks of the centralizer that Brauer correspond to the block of the original character (so in particular have the same defect group).

Corollary

- A representation of defect zero must have value zero on every element whose order is divisible by p
- Because a group with a normal p-group has no blocks of defect zero
- So all the generalized decomposition numbers must be zero.

Middles should do something here

- But I don't know what.

Representations – Theory and Practice – Lecture 18

Representations and characters on a computer

Computers and finite fields

- Computers are quite suitable for working in finite fields.
- Matrix entries do not take up much memory, and you know how much before you start.
- For example a 10,000 x 10,000 matrix mod 2 is 12.5 Megabytes. Very small by today's standards

Adding two vectors is the important thing speed-wise

- For both matrix multiplication and Gaussian Elimination (null-space, split, standard base) you can work with vectors.
- Scalar multiplications can be done (for small fields at least) in advance . . .
- e.g. mod 5 make 1,2,3 and 4 times every row of matrix B and add in the appropriate one.

Characteristic 2

- Adding two vectors is just an "Exclusive Or" operation.
- Modern computers can Exclusive-Or at least 64 bits in one instruction.
- So you can handle huge matrices very fast in characteristic 2.

Larger characteristic

- Over a fairly large prime field (e.g. 1949) you can use the usual arithmetic instructions of the computer to multiply and add, though reduction mod p is usually quite slow and it is best to do that as infrequently as possible

Other tricks available

- Table look-up is good for intermediate fields, especially if they are not of prime order but a prime power.
- That is how the mod-5 worked on Monday.

Mod 3 special trick

- Store 64 entries, with one bit in corresponding positions of two 64-bit registers.
- A sequence of 8 instructions will do the "obvious" add-and-reduce of (0,1,2) accumulated into (0,1,2,3)

8 instruction method

- Can add two 1-bit numbers to get a 2-bit answer using “and” (&) and “exclusive-or” (^)
- These can be combined (using the fact that the input is at most 2 and that 4 = 1 mod 3) to make a 8-instruction accumulate-mod-3 sequence.
- (no-one would ever use that)

7-instruction add mod 3

- But multiplication in the field of order 4 can be done in seven instructions!
- (ax+b)(cx+d) needs four “And” instructions and one “Xor” to get px^2+qx+r
- And $x^2=x+1$ so we need 2 more Xor instructions to reduce mod x^2+x+1
- ☺

Can you do it in six?

- Yes, you can. There are none that use the same encoding for everything
- But A+=B with A in one encoding and B in another works fine.
- 1 and 2 are always represented as 01 and 10
- But zero is encoded as 00 in format A and 11 in format B.

Adding mod 3

R + C = S R=(r1,r2) C=(c1,c2) S=(s1,s2)

x=r1+c2, y=r2+c1 z=x+c1 t=y+c2 s1=y&z s2=x&t

r1	***r2***	***c1***	***c2***	***x***	***y***	***z***	***t***	***s1***	***s2***	***R+C=S***
0	0	1	1	1	1	0	0	0	0	0+0=0
0	0	0	1	1	0	1	1	0	1	0+1=1
0	0	1	0	0	1	1	1	1	0	0+2=2
0	1	1	1	1	0	0	1	0	1	1+0=1
0	1	0	1	1	1	1	0	1	0	1+1=2
0	1	1	0	0	0	1	0	0	0	1+2=0
1	0	1	1	0	1	1	0	1	0	2+0=2
1	0	0	1	0	0	0	1	0	0	2+1=0
1	0	1	0	1	1	0	1	0	1	2+2=1

How about 5 steps?

- There are no sequences of 5 operations that work. I tried them all.
- But I do not know how to prove that you can’t do it in 5½
- In other words add in two numbers in 11 operations
- Actually I can’t even prove you can’t accumulate two of them in 10 (9? 8? 7?) operations
- All I can show is that you need at least 2 operations on average. ☹

Research problem

- There should be some sort of theory that values the information reduction (for adding a lot of numbers together mod 3)
- You start with 3^n possible states
- And then you do some work (and, or, xor)
- And after a few of these you must have at most 3^{n-1} possible states.
- But I have failed to get anywhere with this.

Gaussian elimination

- 1 2 5 3 0
- 0 4 1 2 1
- 0 1 0 2 2
- Is this a linear combination of the above rows, and if so – what linear combination
- 1 8 6 9 5

Gaussian elimination middle

- 1 2 5 3 0
- 0 4 1 2 1
- 0 1 0 2 2
- ==========
- 1 8 6 9 5
- Looking at the first column, it certainly has exactly one of the top row.
- So subtract it off and you are left with
- 0 6 1 6 5
- We can ignore the top row now.

Rest of it

- 0 4 1 2 1
- 0 1 0 2 2
- ==========
- 0 6 1 6 5
- Looking at the third column, we see that the top row must be there exactly once
- So subtract it off
- 0 2 0 4 4. Looking at the second col - 2

Pivots

- **1** 2 5 3 0
- 0 4 **1** 2 1
- 0 **1** 0 2 2
- The big entries are called “pivots”. They are 1, and all entries below them are zero.
- If you have a pivot in each row it is easy to solve linear equations

Gaussian elimination

- So change your matrix so that there ***is*** a pivot in each row!
- This is done with row operations
- i.e. multiplying on the right by a matrix.

Computing with character tables

- The first problem is how to hold the irrationalities.
- The first practical system was CAS, developed in Aachen in the 1970’s
- It held all irrational numbers as explicit sums of roots of 1 (modulo the cyclotomic polynomial.

CAS irrationalities

$(X^8-1)=(X-1)(X+1)(X^2+1)(X^4+1)$

So (X^4+1) is the cyclotomic polyomial

So CAS would hold $a+bX+cX^2+dX^3$ would hold where $X^4=-1$ for any irrationality involving 8^{th} roots of 1

Integral basis is possible

- In fact, it is rather seldom in practice that one wants the roots of 1.
- For example in A5 we needed b5 =(–1+sqrt(5))/2, not the 5^{th} roots of 1.
- This is because if f is an element of order 5 in A5, it is conjugate to its 4^{th} power.

A little Galois Theory

- The automorphism group of the field of n^{th} roots of 1 is the *multiplicative* group of numbers coprime to n mod n.
- Take any subgroup of that (Abelian) group
- And the numbers it fixes form a field.
- All fields generated by character values are of this type.
- The numbers mod n in the subgroup are the powers of itself that it is conjugate to.

(n,[h1,h2…]) notation

- Hence we may name a field of this type by giving n, and the generators h1, h2 …of the fixing multiplicative subgroup.
- For example the b5 field is given by (5,[4]).
- Or sqrt(7) is in (28,[3]).
- Some obvious elements are obtained by taking a (not-necessarily primitive) n^{th} root of 1 and adding up its distinct images under H.
- Thompson [again!] proved that there is always a subset of these orbit sums that form an integral base.
- (Wheras I had just checked it for n < 1,000)

Using an integral basis

- You can store one element's values as a string of ordinary integers
- Which enables you to work with a character table that is a square matrix of ordinary integers.

Ordinary tables

- You can work out reductions of characters using the inner products
- So this is relatively easy.
- This is what CAS did.

Modular tables

- There are no inner products
- So you have to solve linear equations to find out how a character reduces.
- This is possible, but needs a lot more thought.

Representation theory and practice

Lecture 19 – Integral matrices.

Solving linear equations over the integers.

P-adic expression

Finding a vector

What can we do with matrices of integers

- Many people wish to invert a matrix that is invertible.
- Or at least put it into an echelon form-like thing.

1 3 2 4 3 5 4
0 3 1 2 2 1 1
0 1 0 6 8 7 9
0 0 0 8 5 7 6

This has some advantages

- You have to do the work just once and then your “space” is in good shape
- BUT in general the intermediate results can get very big,
- And although there has been much work to make the algorithm practical
- I feel it is the wrong direction for use with character tables and group representations.

The problem I try to solve

- Without changing the matrix at all
- Solve the problem of finding a linear combination of the rows of the matrix that comes to the given row.
- This is suitable for character tables, where you ***really*** do not want to change the matrix!

Meataxe over integers

- But in the end we would also like to be able to work with group representations over the integers.
- Tensor them, split them into irreducibles etc.
- (Also, perhaps make the numbers smaller)

Memory for big numbers

- All the main bignumbers packages allocate memory for the answers of individual calculations
- This makes both the interface and the implementation problematic
- I observe that there is a sub-class of algorithms that can work with lists . . .

Integral meataxe can work with lists

- You have (say) ten ***huge*** registers – a megabyte, say) and (say) five lists of numbers.
- For any arithmetical work, the answer always goes into a register.
- All you can do to write them is to add them to the end of a list.

Several programs are now easy.

- Transpose
- Add
- Matrix multiply
- Once you have your list-processing big numbers these are no problem.

But what about . . . ?

- Rank
- Nullspace
- Split
- Standard basis
- Invert
- How do we do Gaussian Elimination?

Three main methods

- **Approximation.** Hold "real" numbers to a certain number of decimal (actually bicimal) places. Guess the answer and check it.
- **Chinese** – work modulo lots of primes and put the answer together using the Chinese Remainder Theorem. Again guess the answer and check it.
- **P-adic** – work mod p and then divide by p. No guesswork involved for integral work.

P-adic expression.

```
     Integral                Mod 3
 1   3   3   5   2          1 0 0 2 2
 6   4   6   4   2          0 1 0 1 2
 3   3   4   2   1          0 0 1 2 1
==================
 1   1   1   5   2 ??       1 1 1 2 2
       (is the sum of the three rows)
10  10  13  11   5  subtract, divide
-3  -3  -4  -2  -1          0 0 2 1 2
```

Integral expression

- Given a matrix M and a vector V
- ***If*** V is an integral linear combination of the rows of M, find that integral linear combination.
- Work mod p (e.g. 1949)
- Express V as a linear combination mod p
- ***Lift*** the mod p expression to the integers
- Subtract and divide by p
- And go round again. (and stop if V==0)
- Research problem – what properties of the integers am I using here?

This is not much good so far.

- It does enable "invert". Express the rows of the identity matrix as linear combinations of the rows of the given matrix.
- It will not allow rank, split, nullspace, standard basis. . .
- Because a vector may be in the Q-span but not in the Z-span.

Need the rationals

2 3 2
3 2 3
======
1 1 1 What linear combination is this?

Notice that five times the last row is the sum of the two previous, and is therefore ***rationally*** dependent.

So we need to notice somehow to multiply the last row by 5 to see the linear dependence.

Rational expression

- So what would happen if we express 1 1 1 as a linear combination of
  3 2 3 and
  2 3 2 ???

Suppose we used mod 3, so we think it is minus the sum of the two rows.

We subtract getting 6 6 6, then divide to get 2 2 2, which is their sum (mod 3), so we get -1 -1 -1, then -2 -2 -2 then back to 1 1 1. . .

What do you get?

- You get the base-3 expansion of the fact that it is 1/5 of the sum of the two rows!
- So how to you get the number 5?
- You use continued fractions (Euclid's algorithm) on the base 3 numbers!

Suppose we had used p = 10

v = 0.285714…*v1 + ...
So 3.v = 0.857142…*v1 + …
4.v = 1.142856…*v1 + …
7.v = 1.999998…*v1 + …

(so 7.v looks like it might be in the space)

Key step is “find integral basis”

- Given a set of rows in a matrix M
- Find a smallest set of rows that are
  - Integral linear combinations of the rows of M
  - *And* the rows of M are integral linear combinations of the rows found

How do we find integral basis

- Take each row of M in turn.
- Check to see if it is linearly independent and just append if it is.
- Otherwise express it (rationally) in terms of the current basis.
- Then change the current basis so that the index is reduced.
- Can usually reduce to 1.

One problem

- It may happen that some rows are independent, but dependent mod 1949.
- The simple answer is to change prime
- I never got around to implementing that.

- Basically this happens when coincidentally 1949 divides the determinant of something.

Typical situation

- 98347479933487.v = 3452342341324.v1 - 763272396243.v2 + 4345320364874.v3
- If the G.C.D of the first number (98…) and one of the others (e.g. 34…) is 1.
- We can find v1’ = a.v + b.v1 such that
- (98…).v1’ = (98…).a.v + (98…).b.v1
- = (34…).a.v1+(98…).b.v1 + x.v2+y.v3
- = 1.v1 + x.v2+y.v3
- Hence our new space spans all the old vectors and has (98…) times as many vectors as before.

It can get a bit tricky

- 30v = 15.v1 + 10.v2 + 6.v3 . . .

- Need to change ***two*** of the basis vectors.
- That’s not so hard. GCD(30,15) is 15 so
- v1’=v-v1 (so 30.v1’=15.v1+10.v2+6.v3)
- But now we need to check that ***both*** of v and v1 get back into the new space!

So are we making progress

- Yes.
- The measure of progress to use is the index of the current basis we have in the space spanned by all the vectors we are using so far.
- We need to be sure that this number goes down every step
- It does.

With "find free basis"

- We can do . . .
- Nullspace
- Split
- Actually split ***does*** standard basis
- So we can now work with representations of finite groups over the ordinary integers.

But how to find a vector in an invariant subspace.

- In practice if you take the null-space of lots of "small" elements of the integral group algebra, you seem to find one in end.
- I have found no theoretical reason why this should be so.
- Research topic. Understand this. In particular study the rank in the group algebra of A+B+C for three elements A, B, C of the group.

Inverse Galois connection?

- The matrices A+B+C can be left and right multiplied by group elements without changing the rank.
- So we can make C = 1 and get A+B+1
- We can still conjugate
- So we are interested in orbits of G on pairs of elements.
- Which is exactly what inverse Galois theory people are interested in!

Actually there is no real problem

- Compute A+B+C whatever it is
- Find the characteristic polynomial
  - That is a whole subject in itself
- Factorize that polynomial over the integers
  - That is also a whole subject in itself
- Evaluate one factor and find the nullspace of that.
  - Which is, on the face of it, quartic, but *maybe* there is a cubic method having done the characteristic polynomial work
  - So I suspect this is a whole subject in itself also.

Representations – Theory and Practice – Lecture 20

Integral meataxe demonstration.

Representations of A7 over the ordinary integers.

Character table of A7

	2520	24	36	9	4	5	12	7	7
p	power	A	A	A	A	A	AA	A	A
p'	part	A	A	A	A	A	AA	A	A
ind		1A	2A	3A	3B	4A	5A	6A	7A	B**
+		1	1	1	1	1	1	1	1	1
+		6	2	3	0	0	1	−1	−1	−1
o		10	−2	1	1	0	0	1	b7	**
o		10	−2	1	1	0	0	1	**	b7
+		14	2	2	−1	0	−1	2	0	0
+		14	2	−1	2	0	−1	−1	0	0
+		15	−1	3	0	−1	0	−1	1	1
+		21	1	−3	0	−1	1	1	0	0
+		35	−1	−1	−1	1	0	−1	0	0

Some remarks before starting

- Character table is complex irreducibles.
- In fact the 10s can be written over the sqrt(-7) field, and the rest over the rationals
- Complex equivalence and rational implies rational equivalence
- But integral equivalence is stronger

Integral equivalence?

- Hence there are in general several different integral representations that are rationally equivalent.

Only have integral meat-axe

- I haven't got a system that works over the sqrt(-7) field, so we will have to improvise a bit.
- No difficulty in principle – still a P.I.D.
- Let's see how we get on.

Representation theory and practice

Lecture 21 - Fast handing of large matrices over finite fields

Gaussian elimination comes down to matrix multiply

Matrix multiply depends mainly on add

Grease is an important tool

Add uses special tricks for 2 and 3

After that adding and reducing is best

My view of computing in the 2010s

- Computers are getting cheaper, bigger and more numerous
- But ***not*** getting much faster.
- We are at the beginning of the era of learning how to chop up our problems
- But although I know how to do that for the meataxe, there is today no coherent system for implementing the methods in.

Matrices mod p is a big subject

- Conference in Edinburgh last year (this is an edited version of my talk there) on "Matrix Recognition"
- What is the group generated by these matrices.
- They are getting quite good at it.

Overview of computing with finite field matrices

- Chop up big problems into “managable” sizes – hundreds of megabytes, say.
- Reformat matrices for efficient working
- Pre-compute lots of rows of C (grease)
- Performance comes down to speed of vector add in the end.

Large matrices

- Can be chopped into smaller ones in both the horizontal and vertical directions.
- So for example a 30,000 x 30,000 matrix can be chopped into nine 10,000 x 10,000 ones, the work done on them (whether matrix multiply or Gaussian elimination)
- Then stick the answers back together at the end.

Chopping up matrix multiply

- Is easy
- Chop things up how you like
- Obvious method works
- Can do all n^3 multiplications in parallel
- Usually better to be a bit less extreme to save on filespace and I/O time

Gaussian elimination

- If you chop your matrix in both directions, the main work is to “clean” the pivot columns below the pivots
- Which is done by extracting the columns then doing a matrix multiply (then subtract)
- Hence the performance of Gaussian elimination depends on the performance of matrix multiply
- Only quadratic parallelism.

Never implemented

- The chopped-up Gaussian elimination has never been implemented.
- This is because there is no suitable programming language for submitting jobs.
- I hope to fix that within a year or two.

For matrix multiplication, (like any binary function)

- You do as much work as you can that depends on only one input
- And as little as possible that depends on both inputs.
- In this case there is reorganization and reformatting that can be done first.
- This becomes even more worthwhile if you are using it lots of times
- (Which in the chopped-up world, you are)

So to do fast multiplication

A = B x C Suppose we store in format ***D***

- B1 = F1(B) [***D*** → ***B***]
- C1 = F2(C) [***D*** → ***C***]

- A1 = F3(B1,C1) [product in format ***A***]
- A = F4(A1) [***A*** → ***D***]

Why reformat?

- To take advantage of "grease"
- To enlarge the set of possible algorithms.
- So that access to the data is faster for the computer.

What is grease?

- When computing A = B + C
- You compute lots of rows from C (by adding and/or scalar multiplication
- So that when you come to do the actual matrix multiplication
- You can just add in a few rows you already made!

Example - Grease level 2 over F3.

```
..02..      ....................
..10..D     1220021211 1...  D
..01..      2011012110 2...
..11..      ....................
==  B  == x ======== C ==========
 .  2       2011012110 2....
 .  3  B    1022021220 1....  C2
 .  1       1220021211 1....
 .  4       0201000021 0....
 .  .       ....................
```

Some idea of the scope of grease

- Mod 2 – often compute all 512 combinations of nine rows of C. One add then does 9 rows [Grease level 9]
- Mod 3 243 combinations of five rows. One add then does five rows [Grease level 5]
  - Actually with the special formats, multiplication by 2 mod 3 can be done by swapping the registers, so only need 121 rows.

Some idea continued

- Mod 7, we may store 343 combinations of three rows [Grease level 3]
- Mod 127, we may store all 126 multiples so that we only have to add, not multiply. [Grease level 1]

Grease level can be a rational number

- e.g. mod 1949 should use grease 1/2
- Store v, 2v, 3v, . . . 45v (43x46>1949)
- Also 46v, 2.46v, 3.46v . . . 42x46v
- So to add in 131.v you add in
- 2.46v and 39v (2x46+39=131)
- Two adds is still much faster than a multiply (and reduction)
- Real gain is you reduced e.g. 7.46v first.

Wider range of algorithms

- Example – the mod 3 method I showed earlier – need to reformat the matrix C first, since it represents zero by 11.
- Actually we had to reformat C anyway to put the bits in corresponding positions.

Wider range of algorithms

- Example – field of order 27.
- File format (D) has one entry per byte as $9a+3b+c$ for ax^2+bx+c
- But we want each entry to occupy corresponding bits of six registers – loads of bit shuffling.
- But however awful this is, it is quadratic – not cubic.

Wider Range of algorithms

- Example – **the field of order 32.**
- ***D*** (file format) has one entry per byte, using 5 bits.
- For ***C*** take 64 [actually word length] entries and put them into 5 words (p,q,r,s,t) so that, for example, the fifth field entry is bit 5 of each of p, q, r, s and t.
- (for ***C2***, perhaps make 35 non-zero linear combinations of p,q,r,s and t (31, but four of them twice to "go round again")
- For ***B***, hold where to start, adding five consecutive rows of ***C2*** in to the five rows of ***A***. Hold five zero rows somewhere too – faster to add in zero than decide not to
- ***A*** looks muck like ***C*** – at least as far as the addition and scalar multiplication is concerned.

Make data access sequential

- Divide A and B into vertical strips and C into squares
- Grease a single square of C (Cij say)
- (fill your cache with grease)
- Then do the operation that uses Cij – the i-th strip of A and the j-th strip of B.

A = B x C The different formats.

- ***A*** – the format the answer comes out in
  - Suitable for accumulating into.
- ***B*** – the format matrix B should be in
  - Just a set of indexes into the grease table.
- ***C*** – the format matrix C should be in
  - ***C1*** Whole matrix ready to build grease table.
  - ***C2*** Partial matrix fully populated grease table.
- ***D*** – the format in the files.
  - Same as for last 30 years.

Adding mod p

- Adding depends on the characteristic – the degree of the field need not affect it.
- Hence to add in the field of 27 elements, you add the coefficients mod 3.
- Although there is the table-look-up . . .

Table look up

- Store as many entries into a byte (8 bits – 0-255) as you can, and then
- To add two such bytes get ad[256*b1+b2]
- 256*b1 is, of course, a shift, not a multiply
- And the table occupies 65,536 bytes, which these days fits into L2 cache memory
- But this needs the fetch of b1 and b2 and the storing of the (byte) answer separately so these days this is not so good. About 9 operations per byte

Mod 2

- Xor of 8 bytes at a time takes a single operation, though if course there is still the fetch, increment, store etc. In any case it averages less than 1 operation per byte.

Adding mod 3

R + C = S R=(r1,r2) C=(c1,c2) S=(s1,s2)
x=r1+c2, y=r2+c1 z=x+c1 t=y+c2 s1=y&z s2=x&t

r1	***r2***	***c1***	***c2***	***x***	***y***	***z***	***t***	***s1***	***s2***	***R+C=S***
0	0	1	1	1	1	0	0	0	0	0+0=0
0	0	0	1	1	0	1	1	0	1	0+1=1
0	0	1	0	0	1	1	1	1	0	0+2=2
0	1	1	1	1	0	0	1	0	1	1+0=1
0	1	0	1	1	1	1	0	1	0	1+1=2
0	1	1	0	0	0	1	0	0	0	1+2=0
1	0	1	1	0	1	1	0	1	0	2+0=2
1	0	0	1	0	0	0	1	0	0	2+1=0
1	0	1	0	1	1	0	1	0	1	2+2=1

Mod 3

- This adds in 6 operations, but that does a whole word of adds – 8 bytes. Hence this runs at about one operation per byte.

Mod 5

- Use add of a 64-bit number, and occasional and-shift-add to reduce
- (Use 64 = 4 mod 5)
- So store every entry in *seven* bits (so nine of them per 64-bit word)
- Can then do 15 adds without worrying, as 15*4 is only 60.
- Then “and” with 64, “xor” to clear that bit, shift right four places then add
- So reduction step is only needed every 15 adds.

Adding – moderate primes

P	Bits	/64	Adds	Reduction
5	7	9	15	64=4
7	8	8	21	128=2
11	9	7	25	256=1+2
13	10	6	41	512=1+4
17	10	6	31	512=2

Last row means mod 17, each entry takes 10 bits so you store 6 entries in one 64-bit word. You can add 31 times for each reduction, and to reduce, you "and" with 512, "xor", shift right 8 places and "add".

Mod 3 is faster the first way

- Using 6 bits, 32=2 mod 3 adds 10 entries at a time and needs 4 operations every 15 adds so does 150 adds in 19 operations.
- Other way does 64 adds in 6 operations.
- Quite close, really.
- first way is also much tighter on (cache) memory and can negate by swapping words, so is in fact quite a bit faster.

Mod 5

- If you can add mod 5 in 8 operations, that would be good. Should probably look.
- But I'm not really interested in adding mod 5 in 9 operations because . . .
- If there were, it would be about the same speed as adding in 7 bits.
- 135/19 = 7.10523
- 64/9 = 7.11111

Mod 7

- 13 operations is easy – multiply in GF8
- 64/13 = 4.92
- Addition in a byte is much faster
- 168/25 = 6.72

Moral of the story

Computers have good electronics for addition, so use it.

Try to avoid reduction

- For example 1949 use 16 bits per entry
- Usually just add the next number in
  - SSE-2 can do 8 of these in 1 operation
- Every 15 adds (say) reduce it *a bit*
- "and" with 32768, shift right 15 places, multiply by 1584 and add.
  - SSE-2 can do these operations 8 at a time too
- Only at the very end do you bother to get the answer right by doing a (slow) %1949.

23^5 ??

- Grease to level "1/5", - all 23 multiples.
- So needs five adds per entry
- Should do one matrix entry every 5.2 cycles
- Or about 2 seconds for 1000 x 1000. ***in theory***
- But my defined format is a+23b+529c . . .
- And getting to and from that is slow ☹

Faster Access to the data

- The grease table ***C2*** is accessed randomly, so it is quite important that it fits into L2 cache.
- This usually implies cutting a large matrix C up in both directions so that the "little square" of C can be heavily greased, used and discarded.
- A and B are then stored (as parts of rows and indexes into the grease table respectively) so that all the data for each such little square is together and accessed sequentially.

Example ***C2*** – mod 2

- Chop matrix C up into 256 x 512 "squares"
- Row chunk is 64 bytes
- Grease level 8
- 32 "slices" of 8->256 rows – 524,768 in L2
- So chunk add is perhaps 8 x 64 bit Xor
  - Row being added into resides in L1 cache
  - Quite a bit of work per fetch of a ***B*** index and Read and Write-back of ***A*** chunk

Meataxe matrices are not dense!

- Naively implemented, all this stuff was not much faster than the old methods (which did not chop the rows up).
- The old methods took advantage of the large number of zeros there often are in matrix B
- We can do that if a whole load of consecutive B-entries are zero
- Or if a whole Square of C2 is zero for that matter.
- Then the new methods are indeed much faster.

HPMI

- High Performance Meataxe Interface
  - Not properly implemented yet.
  - Beth had a go at quite a bit of it.
- Run time, first job is to decide on a strategy (grease level, sizes of chunks etc.)
- Read matrix B then convert into format ***B***
- Read matrix C then convert into format ***C***
- Do A = B x C on the most suitable formats
- Convert format ***A*** back to ***D*** and write out.

Useful even for small matrices

- Consider format ***B*** (respectively format ***C***) as a format suitable for multiplying on the right (respectively on the left)
- Suppose you wanted to make 100,000,000 matrices . . .
- Would 10,000 Bi x 10,000 Cj do?
- Convert all Bi into a format ***B*** first
- Then grease each Cj in turn (i.e. make ***C2***)

"Multiply and Add"
A += B x C

- This is the performance critical operation of the meataxe for large matrices.
- Multiplication can obviously use it (A=0).
- Gaussian elimination can also utilize this operation for its performance-critical parts
  - Must use the proper echelon form

Layers (in my dreams)

- Fiddling with bits (256 x 512)
  - Need about a megabyte of L2 cache
- Doing a memory full of work (64K x 64K)
  - About 5 minutes in a couple of Gigabytes.
- Local disk worth of work (256K x 256K)
  - 64 of these – ideally about 16 cores taking 20 minutes.
- Doing a file-server's worth of work (2M x 2M)
  - 512 of these – ideally about 50 machines taking a few hours.
- So surely 2M x 2M matrices mod 2 in 1 day!

But

- I do not know a language to code this up in!
- I think I know what to do, though.

- A supercomputer is a device that turns
  - A compute-bound problem into
  - An I/O bound problem
- ☹

Big A += B x C

- At the larger levels, chop each of A, B and C up into **m** pieces in both directions.
- Then do **m**^3 operations A_{ik} += B_{ij} x C_{jk} on the smaller pieces.
- Stick the **m**^2 pieces A_{ik} together again at the end.

Gaussian Elimination needs the "Echelize" routine.

Input – one matrix M.

Output – three matrices – Q1, Q2, R – and a list P of columns.

Puts M into echelon form, and outputs Q1 as the row operations done – Q1.M is in echelon form.

Q2 is the nullspace found as it goes – Q2.M = 0.

P is the list of columns where the pivots are

R is the rest of the matrix.

Small Echelize

- Start with matrix R = M and Q = identity.
- For each i, do row operations to make the first remaining non-zero column have 1 in the i'th row and zeros in all other rows.
- Keep note (in P) of the columns used
- When remaining rows all zero, stop and output P, Q and R.
- Output top and bottom half of Q in separate files Q1 and Q2.

Echelize is recursive

- To echelize a big matrix . . .
- Chop it into pieces (a x b, say)
- Use echelize a.b times on smaller things
- And also uses multiply and add a lot (so this is performance critical
- Other administrative routines . . .
- And then stick the bits together at the end.
- Complex but possible

Pivot files

- New type of meataxe file – a list of pivots – an r x c matrix with each row having a 1 in position Xi in an otherwise zero row.
- The Xi must be in increasing order.

Pivot Extract

- Input and output are format ***D***.
- Selects a particular sequence of columns according to the pivot list P.
- I believe this output should be negated.
- Also output the non-pivotal columns.

Pivot combine

- Combine two (or more) pivot files.
- Most numbers must be renumbered
- The pivot lists are merged.
- Can also merge the rows of matrices in the same way at the same time.
- If properly designed, works with one entry or row at a time and does not need chopping, even in big cases.

Finding Imprimitivity and Tensor factorization

- Doesn't look at all easy in general
- If elements of order fairly large compared to the degree can be found
- We can afford to look through all vectors in an eigenspace and we should be OK
- Imprimitivity is easy once this is given
- Tensor is not so immediate. W.I.P.

Clifford Theory statement

Lecture 22 – Clifford Theory

- If G has a normal subgroup N, the irreducible representations of G are all induced from tensor products of the normalizer of an irreducible of N with a projective representation of the inertial quotient.

Normalizer of an irreducible

- Given any representation (an irreducible representation of N, say) there is the set of matrices (in a particular field) that normalize it.
- This includes the matrices you start with
- And of course ***all*** the scalars
- And quite probably more besides since you may be able to ***some*** automorphisms of the group without changing the representation.

Inertial group

- Given an irreducible of a normal subgroup N, some elements of G may do automorphisms that fix that irreducible, and some may not.
- Those elements of G that fix the irreducible are called the inertial subgroup of that irreducible.
- It contains N as a normal subgroup, so there is an inertial quotient.

Hazard

- If you tensor two representations together, in particular you tensor the centre. Hence the group you get might be different from the one(s) you started with.
- Clifford theory is really a theorem about ***projective*** representations, or representations of groups given only the structure of the central quotient.

Example of hazard

- The group SL(2,5) of 2x2 matrices mod 5 of determinant 1 is 2.A5. It has order 120 (A5 has order 60) and there is a 2-1 map onto A5.
- 2.A5 has two 2-dimensional complex representations X and Y, say
- A5 has a 4 dimensional representation. It is the tensor product of X and Y.

M-algebras – research topic.

- Given generators of an irreducible matrix group (on a computer) find out whether the matrix representation is

a) An induced representation and/or

b) A tensor product

Idea of method

- Look for ***M-algebra***s - sets of matrices ***normalized*** by conjugation and closed under addition and matrix multiplication.
- Definition. Given a representation ρ of a group, an ***M-algebra*** is a set of matrices such that
- $\rho(g^{-1}).m.\rho(g)$, m_1+m_2 and $m_1.m_2$ are all in M

Why look at M-algebras?

- If ρ is the tensor product (of a and b, say) then the set of matrices $I_a \times Z_b$ for all Z_b is an M algebra. Similarly with a and b interchanged.
- If ρ is induced, then there is a direct sum decomposition of the space into disjoint subspaces that are permuted by ρ. The set of all matrices fixing (setwise) each of these spaces is an M-agebra.

Clifford theory (as it ***should*** be)

- I believe that one can prove a theorem about M-algebras – they are all induced from tensor products.
- [Hazard – tensor product of bigger groups]
- So start with this – the fundamental theorem of M-algebras.
- Wedderburn's structure theorem (Closed under + and x => full matrix algebra – ish) does much of the work.

Now suppose G has a normal subgroup N

- Then the restriction of the representation to N gives a set closed under matrix multiplication.
- Close it also under addition and you get an M-algebra
- Which, from the (unproved and unstated!) M-algebra theorem, must therefore be an induction of a tensor product.

Back to classical stuff – Clifford Theory

- G is a group, N a normal subgroup of G, every irreducible representation of G is
- The tensor product of a normalizing matrix group and a "projective" representation of the inertial quotient
- Induced up to G.
- Works in all characteristics.

Admission

- I am not very good at tensor products and induced representations.
- I am only too well aware that the following slides leave some things unproven.
- Hopefully you will get a foggy idea of what is going on sufficient for your purposes.

Let's go

- G a group, N a normal subgroup of G, ρ an absolutely irreducible representation of G in any characteristic.
- Restrict the representation of G to N and take a minimal invariant subspace V of N, giving an irreducible representation of N.
- The images of V must span the whole space, since the original representation was irreducible.

First step

- How many different irreducibles to you get by restricting to N?
- You may get several different ones, but all *automorphic* – although they are not equivalent, they can be the same *set* of matrices, permuted by automorphisms.
- It is only which matrices are which elements of N that change.

Examples of first step

- 2x2 has three non-trivial representations of degree 1.
- They can be permuted by the automorphism group (S3) of 2x2.
- They are therefore automorphic representations.
- Similarly the two 3-dimensional representations of A5 can be swapped by the outer automorphism of A5.

So if N is normal

- It may be that restricting to N gives several different irreducibles
- For example restricting the 3-dimensional representation of S4 to 2x2 we get all three non-trivial representations, once each.
- Or restricting the 6 dimensional irreducible of S5 to A5 we get the two 3-dimensional irreducibles of A5, once each.

Second step

- The space decomposes into parts acted on by different irreducibles of N (though they are all automorphic, so not *that* different!).
- And in fact the whole representation is the representation of the inertial group, [acting on the bit corresponding to the irreducible], induced up.

Induced from inertial group.

- I won't confuse you by trying to prove this.
- It is in fact completely obvious one you know what an induced representation is (which perhaps I don't).
- What is true is that if you know the representation on one part, you know it all, so you could even ***define*** induced representations from this observation

So now only one irreducible of N

- One obvious way of making a representation is to take the set of ALL matrices that normalize the irreducible.
- Then every element of the inertial group does something that can be done in the normalizer . . .
- Multiply each inertial group element by the inverse of that . . .
- And the result commutes with N
- So is "obviously" a tensor product

Example

- 6 dimensional representation of S5 restricts to the two 3-dimensional irreducibles.
- Hence we know the representation on A5 already
- And S5 just swaps them.
- So we know the whole representation.

Second example

- 2^3.L3(2), the 2^3 has seven non-trivial 1-dimensional irreducibles.
- Fixing one of these, we get 2^3.S4 – the inertial group.
- We can therefore tensor our normalizer (dimension 1) with any irreducible representation of S4 (or 2.S4 depending on which group 2^3.L3(2) we have)
- And induce it up.
- The degrees are therefore 7,7,14,21,21
- Or 14,14,28 for the other 2^3.L3(2),

More extreme example

- D8 x Q8 has order 64.
- Quotient by the diagonal central 2 and you get a group of order 32
- It is called 2^{1+4}
- Its automorphism group is actually 2^4.S5. Quite big. The 2^4 are the inner automorphisms.

Representations of 2^{1+4}.A5

- 2^{1+4} is the normal subgroup.
- It has 16 linear representations (of 2^4)
- And one faithful representation of degree 4. This needs -1 to be the sum of two squares, but we will work mod 11 (-1 = 1+9) to avoid this complication.

Normalizer

- So what are the 4x4 matrices mod 11 that normalize our 4-dimensional representation of 2^{1+4} mod 11?
- They are the scalars (order 10) and the full automorphism group 2^{1+4}.S5

2 groups 2^{1+4}.A5

- A5 itself has a double cover, as previously mentioned.
- One can therefore form the “circle product” of a group 2^{1+4}.A5 with 2.A5 to get the other one
- (Take the direct product, quotient the diagonal central 2 and take the diagonal part where the two masps to A5 agree)

One 2^{1+4}.A5

- Has a 4-dimensional faithful representation, and the rest are just tensors with A5.
- Hence the degrees are 4, 12, 12, 16 and 20

The other 2^{1+4}.A5

- Gets the tensor product of the 4-dimensional normalizers with the ***faithful*** reperesntations of 2.A5
- Whose degrees are 2, 2, 4 and 6
- Hence the degrees are 8, 8, 16 and 24

Just to confuse matters

- One of the two groups contains A5 as a subgroup.
- It is the one with degrees 8,8,16,24
- The one that uses the double cover of A5 to tensor with!
- Containing A5 as a subgroup does not seem to be of fundamental importance.

Representations – Theory and Practice – Lecture 23

Rational irreducible representations

Integral representations

Rational representations I

- Since the regular representation is written over the rationals
- We can chop that up to get the rational irreducibles, unique because of Jordan-Hölder theorem.
- These may reduce further if we extend the field to the complex numbers.

Rational representations II

- Given a rational irreducible, the set of rational commuting matrices forms a division ring
- The centre (cx=xc for all x) is a field which is always the field generated by the character values.
- The division ring always has dimension s^2 over the centre.
- s is called the (rational) ***Schur index.***

Example

- The quaternion group of order 8.
- Has four linear representations
- And one complex representation of degree 2

$$\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} \quad \text{and} \quad \begin{matrix} i & 0 \\ 0 & -i \end{matrix}$$

- Although all the character values are integral, the representation can only be written over a field where -1 is the sum of two squares.
- Which it clearly isn't in the rationals

Quaternion group

- There is therefore a 4-dimensional rational irreducible that reduces to two copies of the same complex irreducible over the complex numbers.
- The commuting matrices are also dimension 4, being a copy of the rational quaternions – a division ring, as it must be.

-1 the sum of two squares

- Actually -1 is not the sum of two squares in the field Q(i7) [where $(i7)^2 = -7$] either, so although this field is non-real, that is not sufficient.
- Similarly there is a group of order 12 whose 2-dimensional irreducible can only be written in a field where -3 is the sum of two squares.

Another example

- Take the central product of the previous two groups and you get a group of order 48 with a 4-dimensional representation, namely the tensor product of the two representations
- That can only be written in a field where +3 is the sum of two squares
- In this case the indicator is +

Can multiply division rings

- Given matrices for a division ring, can tensor them together
- These are the matrices that will commute with the tensor product of the representations.
- The result will (uniquely) be a full matrix ring over a division ring.
- This “multiplication” is readily defined without needing a group representation.

Another example

- The group 7.18 where the element of order 18 cubes the element of order 7
- Has two faithful 6-dimensional representation whose character field is Q(i3) where $(i3)^2 = -3$
- I believe that the Schur index of this representation is 3.
- (I am not sure, though)

Calculating the Schur Index

- There is a unique rational irreducible containing any given complex irreducible.
- The multiplicity is the (rational) Schur index.
- It therefore divides the multiplicity in any rational representation.
- The regular representation is rational, and the multiplicity is the degree
- Hence the Schur index divides the degree.

Permutation characters

- Any permutation representation is rational
- Hence the Schur index divides the multiplicity in any permutation representation.
- The action of G on itself ***by conjugation*** is another permutation representation
- The multiplicity in that is just the sum of the character values.
- The Schur index must therefore divide that

Indicator "–" implies Schur index even.

- If the indicator is "–", the real Schur index is 2, so the rational Schur index must be divisible by 2.
- Because any rational rational representation is real.

These elementary methods usually enough

- It is "usually" fairly easy to compute the Schur index
- In the "Atlas" the normal situation is that the Schur index is 2 if the indicator is "-" and 1 otherwise
- Feit checked them all. There are a handful of exceptions.

Integral representations

- Any rational representation is equivalent, over the rationals, to an integral representation (usually not uniquely)
- Choose any vector, and take the set of integral multiples of its G-images
- That is a finitely generated Z-module, so has a Z-basis.

Example

- 2-dimensional representation of S3
- [a , b , c] sum zero all integers
- OR also require them to be congruent modulo 3.
- They are different. If you reduce them mod 3 they are different.

Finitely generated has basis

- Any Z-module with finitely many generators has a basis
- Induction on Q-span dimension
- The key fact is that it is true in a rational 1-space – Z is a Principle Ideal Domain.
- If ax=by there is a z=px+qy such that both x and y are multiples of z. zr=x zs=y

  p q has determinant 1 because

  -s r z=px+qy=pzr+qzs so pr+qs=1

Inductive proof

- So now we can proceed by induction
- And if we ever find a vector W that spans no more rationally but spans some more integrally
- We start by looking only at the coefficient of V_1 and apply the above method to find a 2 x 2 matrix of determinant 1 to act on W and V_1 to change the basis so that we can make the outstanding vector be in the Q-span of $V_2, \ldots V_n$
- Induction then gives us a basis for that, which along with V_1 is the basis we seek

General case

- Given any complex irreducible, we know that there is a unique rational irreducible that contains it.
- There is an algebraic extension of the rationals (a field) in which we can write the representation
- [Either take any element that generates a field of degree s over the centre]
- [Or there is a theorem that the n'th roots of 1 will do, where n is the LCM of the orders of the elements of G]

Trouble is

- The algebraic integers of that field may not be a Principle Ideal Domain.
- I actually do not know a representation that cannot be written over the algebraic integers of ***some*** field of minimal degree.
- But that won't do for mathematicians.

I have often wondered

- Whether one can show that reduction modulo p can always be done starting with a rational representation
- Which can be written integrally
- Reduced mod p
- And then look at the constituents afterwards.

Idea of method

- The idea is to use the commuting integral matrices to show that each complex irreducible corresponds to an invariant subspace mod p, provided you first extend the finite field sufficiently to include the eigenvalues of the commuting (mod p) matrices.
- Haven't got it quite right yet.

"Classical" answer is

- Don't use the algebraic integers.
- Instead decide what ideal you want to reduce mod, and then allow yourself to invert any element not in that ideal.
- That gives a principle ideal domain with the correct field of fractions
- Indeed it has just one maximal ideal
- There may be more "integers" than you expected, but that is no obstruction.

Reduction mod p is not unique

- In general there will be many different ways of reducing a complex representation modulo a prime.
- In particular for any modular irreducible constituent there is a characteristic zero representation that reduces with that as the unique bottom composition factor.
- There is also a characteristic zero representation whose reduction is the direct sum of its constituents.

But the constituents are unique

- In some sense, all the different ways there are of reducing a representation modulo p give the same p-modular irreducible constituents.
- But this is only true provided you stick to the same prime ideal dividing p
- For example if you reduce a representation modulo (1+i7)/2, (a prime dividing 2) you may get different constituents than if you reduce the same integral representation modulo (1–i7)/2.
- But changing the integral representation to one equivalent over the field of fractions will ***not*** change the constituents.

Finite class number

- Given a complex irreducible that is rational, there are only finitely many integral representations rationally equivalent to it.
- I do not know the proof, nor the correct generalization
- But I believe that the class number is finite in a wide variety of circumstances.

Representations – Theory and Practice – Lecture 24

Tensor powers

Quadratic forms

Algebras

Tensor square.

- In odd characteristic the tensor square of a representation is the direct sum of the symmetric and the skew-symmetric part.
- For the General Linear Group (the set of all invertible matrices), these two representations are irreducible, but for smaller groups they may not be.

Hands-dirty proof

Tensor square is the set of square matrices X, where G acts by

$\rho(g)'.X.\rho(g)$

If X' = X [respectively X' = –X] then its image under g has that property also so the space of all such is G-invariant.

Hands clean proof

- The action of G on tensor square commutes with swapping the two tensors
- So commutes with the group algebra of the symmetric group S2 on 2 points
- Hence the null-space and image of any element of the group algebra of S2 is G-invariant.
- ***Independent of characteristic***

First two cases of interest

- A trivial representation at the top (iff also at the bottom) of the symmetric square implies that the representation fixes a symmetric quadratic form (more-or-less obviously).
- A trivial representation at the top (iff also at the bottom) of the skew-square similarly implies a symplectic form

Two more cases of interest

- The original representation at the top of the symmetric [respectively skew-symmetric] square implies a symmetric [respectively skew symmetric] algebra (not usually associative)
- i.e. there is a definition of vector multiplication v * w such that (v*w)g = vg * wg

Conversely

- If the original representation is ***not*** a top constituent of the tensor square
- Then there is no g-invariant algebra.

In characteristic 2 quadratic forms are a bit different.

- For the general linear group, the representation has a uniserial structure, with two copies of the skew-square with a copy of the “Frobenius Square” in the middle. (Square all the entries of the matrix - automorphism in characteristic 2).
- If the original representation is self-dual, there is a 1 at the top and bottom of the skew-square.

Quadratic forms in characteristic 2

- What is a quadratic form?
- it is a 1 at the top of the bottom ***two*** constituents.
- In other words we want to know whether the 1 at the top of the bottom constituent is “glued” to the Frobenius square.
- This can only happen if it (the Frobenius square . . .) is in the principle block.

Characteristic 2 indicator

- If there is a fixed quadratic form, the indicator is **+**
- Otherwise the indicator is **−** if the representation is self-dual and **o** otherwise.

Generality about characteristic 2

- In odd characteristic all ways of saying something are the same
- In even characteristic they are ***not*** always the same
- But there is a way of saying it that works in all characteristics.

Quadratic forms in characteristic 2

- In odd characteristic, a quadratic form is q(v) where q(v+w)=q(v)+q(w)+2.s(v,w) where s is a symmetric bilinear form.
- We could, of course, double the bilinear form first and require q(v+w)=q(v)+q(w)+t(v,w) where t is a symmetric bilinear form.
- That works also in characteristic 2.

To find it

- Using the meat-axe, one can find the matrix that conjugates a representation to the transpose-inverse.
- This will be a matrix s equal to its transpose with zero down the diagonal

Finding the quadratic form in characteristic 2

- In fact, in standard base (which was made to find the bilinear form anyway) all the vectors in the basis are images of each other under the group, so
- IF there is a fixed quadratic form
- THEN it has the same value on all the basis vectors
- So try them all in turn to see if they work.

The Spinor-Norm

- In all characteristics, in even dimension, a matrix fixing a quadratic form has as “parity” which is “even” or “odd” being a homomorphism of the group.
- In all characteristics this is the parity of the dimension of the fixed space. It is therefore parity of the nullity of [matrix minus the identity].
- This works in characteristic 2 also.

This can be used to show there is no fixed quadratic from

- Define SN(m) as the parity of the rank of m+1.
- If G fixes a quadratic form, we must have SN(a)+SN(b)=SN(ab).
- So if two matrices of G fail that condition
- There is no fixed quadratic form.
- (Which can't happen outside the principle block ! ?)

Structure of tensor powers

- For the General Linear group, the tensor n^{th} power of the natural representation commutes with the symmetric group on n points (permuting the tensor factors).
- There is therefore a strong connection between the representation theory of the general linear group $GL(n,p^m)$ and the Symmetric Group S_n mod p.

Character formulae

1^3	21	3
1	1	-2
1	-1	0
0	0	3

Here is the "extended" character table of S3 mod 3.

The p-regular part is the modular characters

The rest is some funny stuff.

Character Formulae

1^3	21	3
1	1	-2
1	-1	1
0	0	3

The top row says that the tensor cube mod 3 always has a constituent with character $[\chi(x)^3+2\chi(x)^2\chi(x)-6.\chi(x^3)]/6$

In other words the Frobenius cube comes out of the symmetric cube.

This is the general situation

- Given a modular irreducible of Sn in characteristic p, the rank of the sum over each Young Subgroup (direct products of natural sub-symmetric-group) in that irreducible tell you the character formula for the "corresponding" constituent of the tensor n^{th} power

More is true

- From a closer study of the representation of Sn, once can work out what the entries in that matrix representation are . . .
- And then write a program to take an arbitrary representation and make that piece of the tensor power.

Tensor square

1^2	2	1^2	2
1	1	1	-1
1	-1	0	2
$p \neq 2$		$p = 2$	

So in characteristic 2, $\chi(x^2)$ is a character. (The Frobenius Square).

What are those zero-degree characters

- Actually they are all just tensor products of Frobenius automorphisms of smaller tensor powers.
- This is an aspect of the "Steinberg Tensor Product Theorem".
- And the theory goes on . . .

Defining characteristic

- There is a whole subject of studying the general linear group (and orthogonal group and symplectic group) in the defining characteristic (i.e. in fields of the same characteristic as the group is defined) which is quite well advanced.

S-16 mod 2 is, I believe, not yet completed.

- It follows that the constituents of the tensor 16^{th} power of a representation in characteristic 2 are not yet known.
- I guess that won't worry you.

Final little fact

- A group in the Atlas ${}^3D4(2)$ has a 26-dimensional ordinary irreducible.
- From ordinary character theory it is easy to calculate that its skew-square contains the original representation, but that the totally skew-symmetric cube has not.
- Hence the algebra is skew symmetric, and the Jacobi identity must hold.
- So F4 must exist!