Modular representation theory

(Very) short introduction

Rafał Lutowski

University of Gdańsk

Kraków, 27 April 2019

Complete fields

p-ADIC NORM

Global assumption

p – a fixed prime

p-adic norm

$a = p^k \cdot m/n \in \mathbb{Q}, k \in \mathbb{Z}, p \nmid mn$:

$$|a|_p := p^{-k}$$

Properties of p-adic norm

1. $|a|_p = 0 \Leftrightarrow a = 0.$
2. $|ab|_p = |a|_p |b|_p.$
3. $|a + b|_p \leq \max(|a|_p, |b|_p).$

Completion of $\mathbb{Q}$

Series ($n \in \mathbb{Z}, 0 \leq a_i < p$)

$$\sum_{i=n}^{\infty} a_i p^i$$

Partial sums

$$s_k = \sum_{i=n}^{k} a_i p^i$$

(s_k) is a Cauchy sequence

$$\lim_{k\to\infty} |s_k - s_{k-1}|_p = \lim_{k\to\infty} |a_k p^k|_p = 0$$

Definition

The completion of $\mathbb{Q}$ – the field $\mathbb{Q}_p$ of p-adic numbers.

p-ADIC NUMBERS

Notation

$$x = \sum_{i=n}^{\infty} a_i p^i = [\ldots a_3 a_2 a_1 a_0 . a_{-1} \ldots a_n]_p$$

Note: $|x|_p = p^{-n}$.

2-adic numbers

$$3 = 11_2 \qquad 2.25 = 10.01_2 \qquad \ldots 0101011_2 = (01)1_2 = \frac{1}{3}$$

p-adic integers

$$\mathbb{Z}_p := \{q \in \mathbb{Q}_p : |q| \leq 1\}$$

p-ADIC INTEGERS

PID

Ideals: $(p^k), k \in \mathbb{N}$.

Local ring

Maximal ideal: (p).

Valuation ring

$\mathbb{Q}_p = \mathbb{Z}_p \cup \mathbb{Z}_p^{-1}$

$\mathbb{Z}_p$ is PID + $\mathbb{Z}_p$ is valuation + $\mathbb{Q}_p$ is complete

$\mathbb{Z}_p$ – complete discrete valuation ring

Residue field

$\mathbb{Z}_p/(p) \cong \mathbb{F}_p$.

$\bmod p$ reduction

$\mathbb{Z}_p \to \mathbb{Z}_p/(p), a \mapsto \overline{a}$.

Finite extensions of $\mathbb{Q}_p$

F finite extension of $\mathbb{Q}_p$

$$a \in F, n = (F : \mathbb{Q}_p)$$

L_a – left multiplication by a

$$L_a \in \mathrm{Hom}_{\mathbb{Q}_p}(F, F)$$

p-adic norm extension

$$|a|_p = |\det L_a|_p^{1/n}$$

Integral elements of F

$$\mathcal{O}_F := \{a \in F : |a|_p \leq 1\}$$

Integral elements of F

PID

Ideals: $(\pi^k), k \in \mathbb{N}$.

Local ring

Maximal ideal: (π).

Valuation ring

$F = \mathcal{O}_F \cup \mathcal{O}_F^{-1}$

$\mathcal{O}_F$ is PID + $\mathcal{O}_F$ is valuation + F is complete

$\mathcal{O}_F$ – complete discrete valuation ring

Residue field

$$\overline{F} = \mathcal{O}_F/(\pi) \cong \mathbb{F}_q$$

$\mod \pi$ reduction

$$\mathcal{O}_F \to \mathcal{O}_F/(\pi), a \mapsto \overline{a}$$

FG, $\mathcal{O}_F G$ AND $\overline{F}G$-MODULES

Burnside theorem

$\mathcal{O}_F G$-lattice

$\mathcal{O}_F G$-module, free and of finite rank as $\mathcal{O}_F$-module

Theorem

Let V be an FG-module of finite dimension n over F. There exists an $\mathcal{O}_F G$-lattice $W \subset V$, of $\mathcal{O}_F$-rank n, st. $F \otimes_{\mathcal{O}_F} W = V$.

$F = \mathbb{Q}_2, G = C_2 = \langle c \rangle, V = FG$ - regular module

$$W_1 = \langle 1, c \rangle, W_2 = \langle (1+c)/2, (1-c)/2 \rangle.$$

Basis of W is a basis of V

$\chi_W(g) = \chi_V(g)$ for every $g \in G$

Reduction

$\mathcal{O}_F$-module $\overline{F}$. $a \in \mathcal{O}_F, u \in \overline{F}$:

$$\text{(left)} \qquad a \cdot u := \overline{a}u = u\overline{a} =: u \cdot a \qquad \text{(right)}$$

W – $\mathcal{O}_F G$-lattice, $\overline{W} := \overline{F} \otimes_{\mathcal{O}_F} W$

Mapping $W \to \overline{W}$, given by $w \mapsto \overline{w} = \overline{1} \otimes w$. Module structure

$$\overline{a} \cdot \overline{w} = \overline{a} \otimes w = \overline{1} \otimes aw = \overline{aw}$$

W – $\mathcal{O}_F G$-lattice, $\overline{W} := \overline{F} \otimes_{\mathcal{O}_F} W$, $V = F \otimes_{\mathcal{O}_F} W$:

$$\chi_{\overline{W}}(g) = \overline{\chi_W(g)} = \overline{\chi_V(g)} \text{ for every } g \in G.$$

Idempotents in rings

Idempotent

$$e^2 = e \neq 0$$

Orthogonal idempotents

$$e_1 e_2 = e_2 e_1 = 0$$

(Central) Primitive idempotent:

not a sum of (central) orthogonal idempotents

Decomposition

$e_1, \ldots, e_n$ – primitive orthogonal idempotents of a ring R

$$1 = e_1 + \ldots + e_n \leftrightarrow R = I_1 \oplus \ldots \oplus I_n$$

$I_k = Re_k$ – indecomposable left ideal (left R-module)

Decomposition of a left R-module W

$$W = e_1 W \oplus \ldots \oplus e_n W$$

$c_1, \ldots, c_h$ – primitive central orthogonal idempotents of R

$$1 = c_1 + \ldots + c_h \leftrightarrow R = B_1 \oplus \ldots \oplus B_h$$

$B_k = Rc_k = c_k R$ – indecomposable (two-sided) ideal (block)

DECOMPOSITION: FG VS. $\mathcal{O}_F G$

$F = \mathbb{Q}_2, G = C_2 = \langle c \rangle, \mathcal{O}_F = \mathbb{Z}_2$

Idempotents in FG:

$$1, e_1 = (1+c)/2, e_2 = (1-c)/2$$

$1 = e_1 + e_2, e_1 e_2 = 0$, but $e_1, e_2 \notin \mathcal{O}_F G$.

Reduction/lifting of idempotents

Theorem

Every decomposition of 1 of $\overline{F}G$ to the sum of pairwise orthogonal primitive (central primitive) idempotents

$$1 = u_1 + u_2 + \ldots + u_m$$

corresponds to a decomposition of 1 of $\mathcal{O}_F G$ to the sum of pairwise orthogonal primitive (central primitive) idempotents

$$1 = e_1 + e_2 + \ldots + e_m$$

satisfying $\overline{e_i} = u_i$, for $i = 1, \ldots, m$.

Lift may not be unique: $u \in (\mathcal{O}_F G)^*, \overline{u} = 1$

$$1 = ue_1u^{-1} + ue_2u^{-1} + \ldots + ue_mu^{-1}$$

Reduction/lifting of idempotents

Theorem

$$\mathcal{O}_F G \ni \quad 1 = e_1 + e_2 + \ldots + e_m \quad \leftrightarrow \quad u_1 + u_2 + \ldots + u_m = 1 \quad \in \overline{F}G$$

Corollary

$$\mathcal{O}_F G = W_1 \oplus \ldots \oplus W_r \quad \leftrightarrow \quad \overline{W_1} \oplus \ldots \oplus \overline{W_r} = \overline{F}G$$

$W_i, \overline{W_i}$ – *indecomposable, for* $i = 1, \ldots, r$

Corollary

$$\mathcal{O}_F G = B_1 \oplus \ldots \oplus B_t \quad \leftrightarrow \quad \overline{B_1} \oplus \ldots \oplus \overline{B_t} = \overline{F}G$$

$B_i, \overline{B_i}$ – *blocks, for* $i = 1, \ldots, t$

Reduction/lifting of idempotents: Example

$F = \mathbb{Q}_2, G = S_3$

$a = (1\,2\,3), b = (1\,2)$

$d = 1 + a + a^2$

$d \in Z(\mathcal{O}_F G), d^2 = 3d$

$c_1 = d/3, c_2 = 1 - c_1$

$1 = c_1 + c_2$

Primitive orthogonal idempotents of FG ($c = c_1$)

$e_1 = (1+b)c/2, \quad e_2 = (1-b)c/2 \quad : \quad e_1 + e_2 = c_1$ in FG

$e_3 = (c - a^2)(1+b), \quad e_4 = (1-b)(c-a) \quad : \quad e_3 + e_4 = c_2$ in $\mathcal{O}_F G$

Primitive orthogonal idempotents of $\overline{F}G$

$$\overline{c} = 1 + \overline{a} + \overline{a}^2, \overline{e_3} = (1+\overline{a})(1+\overline{b}), \overline{e_4} = (1+\overline{b})(1+\overline{a}^2)$$

Brauer characters

Assumptions, definitions

F – finite extension of $\mathbb{Q}_p$ + splitting field for G

F – finite extension of splitting field for $x^{\exp G} - 1$ in $\mathbb{Q}_p$

Corollary

$\overline{F}$ – finite extension of $\mathbb{F}_p$ + splitting field for G

$\zeta \in \mu_{p'}$ – primitive m-th root

$\overline{\zeta}$ – primitive m-th root

ζ – primitive p^k-th root

$\zeta = 1+(\zeta-1), |\zeta-1|_p < 1 \Rightarrow \overline{\zeta} = 1$

Corollary

$$\overline{}\colon \mu_{p'} \to \overline{\mu}_{p'} \text{ – bijection}$$

Important case

$H = \langle a \rangle$ – cyclic of order m prime to p

ζ – primitive m-th root of $1 \in FH$:

$$1 = e_1 + e_\zeta + e_{\zeta^2} + \ldots + e_{\zeta^{m-1}}$$

where $ae_x = xe_x$ for $x = 1, \zeta, \ldots, \zeta^{m-1}$:

$$e_x = (1 + x^{-1}a + x^{-2}a^2 + \ldots + x^{-m+1}a^{m-1})/m \in \mathcal{O}_F H.$$

$e_1, \ldots, e_{\zeta^{m-1}}$ – primitive orthogonal and central idempotents.

Over $\mathcal{O}_F H$ and $\overline{F}H$

1. indecomposable module = irreducible module
2. indecomposable = of rank/dimension 1

Brauer character

$\overline{W}$ – $\overline{F}G$-module

Goal: define $\varphi_{\overline{W}} \colon G_{p'} \to \mathcal{O}_F$

g of order m prime to p, $H = \langle g \rangle$

$\zeta \in \mu_{p'}$ – primitive m-th root

$\operatorname{res}_H \overline{W} = \overline{W}_1 \oplus \ldots \oplus \overline{W}_r$

$$\forall_i \exists_{x_i \in \mu_{p'}} \forall_{w \in \overline{W}_i} g \cdot w = \overline{x}_i w$$

Lift of $\operatorname{res}_H \overline{W}$: $\mathcal{O}_F H$-lattice W

$$W = W_1 \oplus \ldots \oplus W_r$$

Brauer character

$$\varphi_{\overline{W}}(g) := \chi_W(g) = x_1 + \ldots + x_r$$

$\overline{W}$ – simple: $\varphi_{\overline{W}}$ – simple

$\operatorname{IBr}_p G$ – set of Brauer characters of simple $\overline{F}G$-modules

Example

$F = \mathbb{Q}_2(\zeta),\ \zeta^2 + \zeta + 1 = 0,\ \mathcal{O}_F = \mathbb{Z}_2[\zeta],\ \overline{F} = \mathbb{F}_2(\overline{\zeta}),\ G = S_3 = \langle a, b \rangle$

Simple $\overline{F}G$-module $\overline{W} = \overline{F}^2, a \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, b \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Eigenvalues of a and a^2: $\overline{\zeta}, \overline{\zeta}^2$

$$\chi_{\overline{W}}(1) = 0 \text{ and } \chi_{\overline{W}}(a) = \chi_{\overline{W}}(a^2) = \overline{\zeta} + \overline{\zeta}^2 = 1$$

but

$$\varphi_{\overline{W}}(1) = 2 \text{ and } \varphi_{\overline{W}}(a) = \varphi_{\overline{W}}(a^2) = \zeta + \zeta^2 = -1$$

Brauer characters: Properties

Lemma

- *Every sum of Brauer characters is a Brauer character.*
- *Every Brauer character is of the form*

$$\psi = \sum_{\varphi \in \mathrm{IBr}_p G} n_\varphi \varphi$$

  where $n_\varphi \in \mathbb{Z}_{\geq 0}$.
- *Every Brauer character is constant on every* p*-regular conjugacy class.*

Brauer characters: Properties

$g \in G, \lvert g \rvert = qm, q = p^k, p \nmid m$	$g_{p'} = g^{lq}$	$g_p = g^{km}$
$\exists_{k,l \in \mathbb{Z}}\ km + lq = 1$	p-regular g-part	p-singular g-part

Lemma

Let $\overline{W}$ be an $\overline{F}G$-module, $\chi_{\overline{W}}$ and $\varphi_{\overline{W}}$ – its character and Brauer character respectively. Then $\chi_{\overline{W}}(g) = \overline{\varphi_{\overline{W}}(g_{p'})}$.

Brauer characters: Properties

Theorem

1. *Brauer characters corresponding to non-isomorphic $\overline{F}G$-simple modules are linearly independent.*
2. *The number of simple Brauer characters iq equal to the number of p-regular conjugacy classes of G.*

Corollary

The set of the simple Brauer characters is a basis of the space of functions which are constant on each conjugacy class of p-regular elements of G.

Theorem

If $p \nmid |G|$ then $\operatorname{IBr}_p G = \operatorname{Irr} G$.

Example: Brauer table for S_3

Step 1: Ordinary character table

	$()$	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Step 2: Drop 2-singular classes

	$()$	(123)
χ_1	1	1
χ_2	1	1
χ_3	2	-1

Step 3: Brauer character table for $p = 2$

	$()$	(123)
φ_1	1	1
φ_2	2	-1

Characters in blocks

Block decomposition

$$\mathcal{O}_F G = B_1 + \ldots + B_r$$

$B \in \{B_i\}$

$$B = \mathcal{O}_F G c$$

FG-simple V

$$V \in B : cV = V$$

$v \in V$

$$c(cv) = cv$$

$\chi_V(c) = \dim V$

$$V \in B \Leftrightarrow \chi_V(c) \neq 0$$

Characters in block

$$\operatorname{Irr} B := \{\chi \in \operatorname{Irr} G : \chi(c) \neq 0\}$$

Example: $\mathbb{Q}_2 S_3$

$$\chi_1, \chi_2 \in B_1, \chi_3 \in B_2$$

Defects of characters

Valuation $\nu_\pi : FG \to \mathbb{Z}$

$$\nu_\pi(x) = n \Leftrightarrow x = \pi^n y, y \in \mathcal{O}_F^*$$

p-defect of character $\chi \in \operatorname{Irr} G$

$$d_p(\chi) = \nu_p(|G|) - \nu_p(\chi(1))$$

B – block, $\chi \in \operatorname{Irr} B$

$$\underbrace{d_p(\chi) = 0 \Leftrightarrow \operatorname{Irr} B = \{\chi\} \Leftrightarrow \chi \text{ – char. of proj. } \mathcal{O}_F G\text{-mod.}}$$

$$\Downarrow$$

$\chi_{|G_{p'}}$ – simple Brauer character of G

Defects: application for $G = S_4, p = 3$

Convention

$$1a = ()^G, 2a = (12)(34)^G, 3a = (123)^G, 2b = (12)^G, 4a = (1234)^G$$

1: Ordinary character table

	$1a$	$2a$	$3a$	$2b$	$4a$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	2	2	-1	0	0
χ_4	3	-1	0	1	-1
χ_5	3	-1	0	-1	1

2: Drop 3-singular classes

	$1a$	$2a$	$2b$	$4a$
χ_1'	1	1	1	1
χ_2'	1	1	-1	-1
χ_3'	2	2	0	0
χ_4'	3	-1	1	-1
χ_5'	3	-1	-1	1

Defects: application for $G = S_4, p = 3$

Convention

$$1a = ()^G, 2a = (12)(34)^G, 3a = (123)^G, 2b = (12)^G, 4a = (1234)^G$$

3: $\chi_3' = \chi_1' + \chi_2'$

	$1a$	$2a$	$2b$	$4a$
χ_1'	1	1	1	1
χ_2'	1	1	-1	-1
χ_4'	3	-1	1	-1
χ_5'	3	-1	-1	1

DEFECTS: APPLICATION FOR $G = S_4, p = 3$

Convention

$$1a = ()^G, 2a = (12)(34)^G, 3a = (123)^G, 2b = (12)^G, 4a = (1234)^G$$

3: $\chi'_3 = \chi'_1 + \chi'_2$

	$1a$	$2a$	$2b$	$4a$
φ_1	1	1	1	1
φ_2	1	1	-1	-1
φ_3	3	-1	1	-1
φ_4	3	-1	-1	1

4: $d_3(\chi_3) = d_3(\chi_4) = 0$ – We've got Brauer character table