Representation theory for unitary groups over finite local rings

Allen Herman (University of Regina)

University of St. Andrews,
November 6, 2014

Abstract

Abstract: Let L be quadratic extension of a p-adic number field K. The ring of integers $\mathcal{O}_L$ has a non-trivial involution induced by the Galois automorphism of L, which induces an involution $*$ on $M_n(\mathcal{O}_L)$ in a manner that reminds us of the conjugate-transpose operation. The resulting unitary group
$U_n^*(\mathcal{O}_L) = \{X \in M_n(\mathcal{O}_L) : XX^* = I\}$.
The congruence subgroup property implies that any continuous finite-dimensional representation of $U_n(\mathcal{O}_L)$ factors through a congruence subgroup. This reduces the study of these representations to that of describing the irreducible representations of unitary groups over finite local rings.
Recently we have calculated the orders of unitary groups of finite local rings in both ramified and unramified cases, and constructed irreducible characters that arise as constituents of the Weil representation of $U_n(\mathcal{O}_L)$. These results rely on tools from Clifford theory and hermitian geometry that we will explore in this talk.

The articles

This is based on joint work with Fernando Szechtman, Rachael Quinlan, and James Cruikshank.

[S'03] F. Szechtman, A family of complex irreducible characters possessed by unitary and special unitary groups defined over local rings, *Comm. Algebra*, **31** (2003), (5), 2381-2401.

[HS'13] AH and F. Szechtman, The Weil representation of a unitary group associated to a ramified quadratic extension of a finite local ring, *J. Algebra*, **392** (2013), 158-184.

[CHQS'14] J. Cruikshank, AH, R. Quinlan, and F. Szechtman, Unitary groups over local rings, *J. Algebra and its Applications*, **13**, (2014), (2), 23 pgs.

Motivation

Representation theory: Want to find the irreducible representations of a group/algebra: these are the surjective algebra homomorphisms

$$\mathbb{C}G \twoheadrightarrow M_n(\mathbb{C}).$$

Unitary groups: The *classical groups* over an integral domain R are: $GL_m(R)$, $SL_m(R)$, $O_m(R)$, and $Sp_{2m}(R)$.
The unitary group U_m is a "conjugate-transpose" variant of O_m, i.e. the isometry group of a hermitian form.

The unitary group $U_m^h(S)$

Let S/R is a Galois extension of degree 2, so S is R-free of rank 2 with nontrivial R-linear ring automorphism $*$.

Let V be a free S-module of rank m. The action of $*$ extends to V entrywise, and the $*$-transpose map is an involution on $M_m(S)$.

A hermitian form on V is a map $h : V \times V \to S$ that is S-linear in the 2nd variable and satisfies

$$h(v, w) = h(w, v)^* \text{ for all } v, w \in V.$$

Our unitary group is the isometry group of this form:

$$U_m^h(S) = \{g \in GL_m(S) : h(gv, gw) = h(v, w) \text{ for all } v, w \in V\}$$

Rings of p-adic integers

Let K be a p-adic number field; i.e. a finite extension of the p-adic field $\hat{\mathbb{Q}}_p$.

Rings of p-adic integers

Let K be a p-adic number field; i.e. a finite extension of the p-adic field $\hat{\mathbb{Q}}_p$.

Let $\mathcal{O}_K$ be the integral closure of the ring of p-adic integers $\hat{\mathbb{Z}}_p$.

$\mathcal{O}_K$ is a complete local ring whose maximal ideal $\pi_K\mathcal{O}_K$ satisfies

$$(\pi_K\mathcal{O}_K)^e = p\mathcal{O}_K,$$

and

$$\mathcal{O}_K/\pi_K\mathcal{O}_K \simeq \mathbb{F}_{p^f}.$$

Quadratic extensions of rings of p-adic integers

Let L/K be a quadratic extension, K a p-adic number field. Then $L = K[y]$, and since $char(L) = 0 \neq 2$, y can be chosen so that

$\mathcal{O}_L = \mathcal{O}_K + y\mathcal{O}_K$,

$y^2 \in \mathcal{O}_K \setminus \mathcal{O}_K^2$, and

the galois automorphism of L/K satisfies

$$(r + ty)^* = r - ty, \text{ for all } r, t \in R.$$

There are two types of quadratic extension here:

unramified: $y^2 \in \mathcal{O}_L^\times$ a unit, or

ramified: $y^2 = \pi_K$ generates the maximal ideal of $\mathcal{O}_K$.

Unitary groups over rings of p-adic integers

This allows us to produce a p-adic unitary group $U_m^h(\mathcal{O}_L)$ given a hermitian form h on $V = \mathcal{O}_L^{(m)}$.
The two types of extension give very different results, as do two different types of forms!

Unitary groups over rings of p-adic integers

This allows us to produce a p-adic unitary group $U_m^h(\mathcal{O}_L)$ given a hermitian form h on $V = \mathcal{O}_L^{(m)}$.
The two types of extension give very different results, as do two different types of forms!

The representation theory of $U_m^h(\mathcal{O}_L)$ is reduced to that of the finite unitary groups $U_m^{\bar{h}}(\mathcal{O}_L/y^n\mathcal{O}_L)$ by

Theorem (Borel - see LNIM no. 267 (1976))

Compact p-adic linear groups satisfy the congruence subgroup property; i.e. every normal subgroup of finite index contains a congruence subgroup.

Quadratic extensions of finite local rings

Let R be a finite local ring of characteristic p whose maximal ideal xR satisfies $x^\ell = 0$ (minimal ℓ), and $R/xR \simeq \mathbb{F}_q$ for $q = p^f$.

Let $S = R[y] = R + Ry$ be a quadratic local ring extension of R, which occurs in one of two ways:

S/R unramified: y^2 is a non-square in R. Then $J = xS$ is the maximal ideal of S, $S/J \simeq \mathbb{F}_{q^2}$, and $J^\ell = 0$.

S/R ramified: $y^2 = x$. Then $J = yS$ is the maximal ideal of S, $S/J \cong \mathbb{F}_q$, and $J^e = 0$ (e minimal) with either $e = 2\ell$ or $e = 2\ell - 1$.

The Main Problem

The long-term goal is to describe the unitary groups $U_m^h(S)$ and their irreducible representations.

When p is odd, we have been able to:

- give a formula for the order of $U_m^h(S)$;
- construct irreducible representations that are constituents of the Weil representation of $U_m^h(S)$, and
- give the degrees of these irreducible representations **when e is even**. (Recall $J^e = 0$.)

When p is odd, S has an involution given by $(r + sy)^* = r - sy$, for all $r, s \in R$.

Let $V = S^{(m)}$ be a free S-module of rank m.

Let $h : V \times V \to S$ be a nondegenerate hermitian form on V; i.e. there is a basis $\{v_1, \ldots, v_m\}$ of V whose associated Gram matrix $(h(v_i, v_j))_{i,j}$ is invertible.

Let $U = U_m^h(S)$.

We say that a vector $v \in V$ is primitive if $v \notin yV$. Only primitive vectors can lie in a basis of V.

An orthogonal basis of V is a basis whose associated Gram matrix is diagonal.

Theorem (CHQS14)

Assume p is odd.

- *Every primitive vector of V lies in an orthogonal basis of V.*
- *If $m \geq 2$ then V has an orthogonal basis $\{v_1, \ldots, v_m\}$ for which the Gram matrix $I_h = (h(v_i, v_j))_{i,j}$ is either* $diag(1, 1, \ldots, 1)$ *or* $diag(1, \ldots, 1, \delta)$ *for* $\delta \in R^\times \setminus R^{\times 2}$.

The δ type of hermitian form can only occur when S/R is ramified, or for symmetric forms over over R.

Note: There are two types of unitary groups. In the above basis, $U_m^h(S) = \{g \in GL_m(S) : g(g^*)^T = I_h\}$.

Computing the order of $U_m^h(S)$

Theorem (CHQS'14)

- *If v, w are primitive in V, then $h(v,v) = h(w,w) \iff w \in Orb_U(v)$.*
- *If v is a primitive vector in V with $h(v,v) = 1$, then $Stab_U(v) \simeq U_{m-1}^{h'}$ where h and h' are of the same type.*
- *(Baeza) The canonical homomorphism $U_m^h(S) \twoheadrightarrow U_m^{\bar{h}}(S/J^n)$ is surjective for all n.*

It is a consequence of these that $|U_m^h(S)| = d(1) \cdot |U_{m-1}^{\bar{h}}(S)|$ where $d(1)$ is the number of primitive $v \in V$ with $h(v,v) = 1$.

The orders of the unitary groups

Theorem

- *If S/R is unramified, then $|U_m(S)| = q^{m^2(e-1)}|U_m(\mathbb{F}_{q^2})|$.*
- *If S/R is ramified then*

$$|U_m^h(S)| = \begin{cases} q^{(m^2(e-1)+m)/2}|O_m^{h'}(\mathbb{F}_q)| & \text{if } e = 2\ell, \\ q^{m^2(e-1)/2}|O_m^{h'}(\mathbb{F}_q)| & \text{if } e = 2\ell - 1. \end{cases},$$

where h and h' are of the same type.

Remark: Formulas for the orders of these classical groups over finite fields appear in Cameron's lecture notes. The groups are available in GAP.

The Face-Saving secret!

The number $d(1)$ when $m = 2$ is the number of squares r in $\mathbb{F}_q$ for which $r - 1$ is a square ($+$-type) or non-square ($-$-type).

The Face-Saving secret!

The number $d(1)$ when $m = 2$ is the number of squares r in $\mathbb{F}_q$ for which $r - 1$ is a square ($+$-type) or non-square ($-$-type). This can be computed recursively for increasing ℓ using an application of *Jacobi sums*:

Theorem (Jacobi sums counting formula)

The number of solutions $(x_1, \ldots, x_r)$ in $\mathbb{F}_q^{(r)}$ to a polynomial equation of the form $a_1 x_1^{e_1} + \cdots + a_r x_r^{e_r} = b \neq 0$ is given by

$$\sum_{\chi_i^{e_i} = \epsilon} \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1})(\chi_1 \cdots \chi_r)(b)\mathcal{J}(\chi_1 \cdots \chi_r),$$

where the sum is over linear characters of $\mathbb{F}_q^\times$, ϵ is the trivial character, and $\mathcal{J}$ denotes the Jacobi symbol

$$\mathcal{J}(\chi_1 \cdots \chi_r) = \sum_{\sum u_i = 1} \chi_1(u_1) \cdots \chi_r(u_r).$$

Constructing irreducible representations of U, part 1

Theorem (Clifford theory - going up version)

Let N be a normal subgroup of a finite group G.

Suppose $\varphi \in Irr(N)$. Let $H = Stab_G(\varphi)$.

Then any $\chi \in Irr(G|\varphi)$ is equal to ψ^G for some $\psi \in Irr(H|\varphi)$.

Furthermore, if φ extends to its stabilizer, then

$$\chi(1) = [G : H]\varphi(1),$$

i.e. the degree of χ is $[G : H]$ times the degree of φ.

Constructing an irreducible representation of U, part 2

Let $\bar{S} = S/y^\ell S$, and let $\bar{U} = U_m^{\bar{h}}(\bar{S})$.

$y^\ell V$ is a totally isotropic subspace of V; i.e.
$h(y^\ell v, y^\ell w) = (-1)^\ell y^{2\ell} h(v, w) = 0$, for all $v, w \in V$.

h induces a hermitian form $\bar{h}$ on the quotient space $\bar{V}$ that is of the same type as h.

Constructing an irreducible representation of U, part 3

Let v be a primitive vector of V.
Define $C(v) = \{g \in U : gv \cong v \mod y^{\ell} V\}$.

Let $\mu : S_+ \to \mathbb{C}^{\times}$ be a linear character of the additive finite group S_+ with maximal order.

The (standard?) construction of the Weil representation of U corresponding to μ reveals that $\beta_v(g) = \mu(h(gv, v))$ defines a linear character of $C(v)$.

We have that $N = \bigcap_{v \text{ primitive}} C(v)$ is a normal subgroup of U. Let $\alpha_v = \beta_v|_N$.

The stabilizer of α_v in U is $B(v) = C(v)\mathcal{N}$, where $\mathcal{N} \simeq \{s \in S^{\times} : ss^* = 1\}$.

Constructing an irreducible representation of U, part 4

Theorem (HS'13)

Let v be a representative of a coset of V mod $y^\ell V$.

- *β_v (hence α_v) extends to $\gamma_v \in Irr(B(v))$.*
- *$\chi_v = (\gamma_v)^G \in Irr(U)$ with degree $[U : B(v)]$.*
- *$[U : B(v)] = [\bar{U} : Stab_{\bar{U}}(\bar{v})]/2q^{\ell - \lceil \ell/2 \rceil}$.*

Actual computation of $\chi_v(1)$ is technical. There are many cases depending on m, e, and $h(v, v)$. We are able to give explicit formulas in all cases where e is even.

For example:
If $m = 2r$, $e = 2\ell$, and $h(v, v) \in R^{\times 2}$, then

$$\chi_v(1) = q^{m\ell - m + r - \ell}(q^r \mp 1)/2$$

depending on whether h is of $\pm$-type.