On the arithmetic of integral representations of finite groups

Dmitry Malinin

Università degli Studi di Firenze

ISCHIA GROUP THEORY 2018

Let R be a Dedekind domain with quotient field K, let H be an R-order, L – absolutely irreducible H-representation module (i.e., a finitely generated H-module that is torsion free as an R-module and such that $K \otimes_R L$ is an absolutely irreducible $K \otimes_R H$-module).
The most interesting case is the case where $H = RG$, G a finite group and $charK \nmid |G|$, it was treated in many classical papers by K. Roggenkamp, D. K. Faddeev, I. Reiner, A. V. Roiter, L. A. Nazarova, W. Plesken, G. Nebe and many others.

Integral representations

Jordan-Zassenhaus theorem:
Every isomorphism class of KG-representation modules splits in a finite number of isomorphism classes of RG-representation modules if the ideal class group of R is finite.

The most interesting questions are:

1. Is it possible to find a reasonable estimate of the number of isomorphism classes?
2. What happens if $cl(R)$, the ideal class group of R, is infinite?
3. Can we describe the representations explicitly?
4. Let R be the maximal order in a number field K. Is it possible to find out whether a representation over K can be realized over R?

Integral representations

Jordan-Zassenhaus theorem:
Every isomorphism class of KG-representation modules splits in a finite number of isomorphism classes of RG-representation modules if the ideal class group of R is finite.

The most interesting questions are:

1. Is it possible to find a reasonable estimate of the number of isomorphism classes?
2. What happens if $cl(R)$, the ideal class group of R, is infinite?
3. Can we describe the representations explicitly?
4. Let R be the maximal order in a number field K. Is it possible to find out whether a representation over K can be realized over R?

Integral representations

Jordan-Zassenhaus theorem:
Every isomorphism class of KG-representation modules splits in a finite number of isomorphism classes of RG-representation modules if the ideal class group of R is finite.

The most interesting questions are:

1. Is it possible to find a reasonable estimate of the number of isomorphism classes?
2. What happens if $cl(R)$, the ideal class group of R, is infinite?
3. Can we describe the representations explicitly?
4. Let R be the maximal order in a number field K. Is it possible to find out whether a representation over K can be realized over R?

Jordan-Zassenhaus theorem:
Every isomorphism class of KG-representation modules splits in a finite number of isomorphism classes of RG-representation modules if the ideal class group of R is finite.

The most interesting questions are:

1. Is it possible to find a reasonable estimate of the number of isomorphism classes?
2. What happens if $cl(R)$, the ideal class group of R, is infinite?
3. Can we describe the representations explicitly?
4. Let R be the maximal order in a number field K. Is it possible to find out whether a representation over K can be realized over R?

Let G be a finite group, K a number field with the ring of integers O_K and $\rho : G \to GL_n(K)$ an irreducible representation of G. We denote by V the associated irreducible KG-module.

Definition.
The representation $\rho : G \to GL_n(K)$ is called integral, if and only if $\rho(g) \in GL_n(O_K)$ for all $g \in G$. We say that $\rho(G)$ can be made integral, if and only if there exists an integral representation $G \to GL_n(O_K)$ which is equivalent to ρ. We call V integral if $\rho(G)$ can be made integral.

In other words, $\rho(G)$ can be made integral if and only if we can apply a base change such that all matrices have integral entries.

Question. *(W. Burnside, I. Schur, later W. Feit, J.-P. Serre). Given a linear representation $\rho : G \to GL_n(K)$ of finite group G over a number field $K/\mathbb{Q}$, is it conjugate to a representation $\rho : G \to GL_n(O_K)$ over the ring of integers O_K?*

There is an algorithm which efficiently answers this question, it decides whether this representation can be made integral, and, if this is the case, a conjugate integral representation can be computed.

Integral representations

Proposition. Assume that one of the conditions hold:
(i) We have $K = \mathbb{Q}$.
(ii) We have $cl_K = 1$.
(iii) We have $GCD(cl_K; n) = 1$.
Then the representation $\rho : G \to GL_n(K)$ can be made integral.

Integral representations

D. K. Faddeev, 1965, 1995. – Generalized integral representations.

Theorem (Cliff, Ritter, Weiss). *Let G be a finite solvable group. Then every absolutely irreducible character* χ *of G can be realized over* $\mathbb{Z}[\zeta_m]$*, where m is the exponent of G.*

Example. The metacyclic group $G = \langle x; y | x^9 = y^{19} = 1; y^x = y^7 \rangle$ admits an absolutely irreducible representation $G \to GL_3(K)$ which cannot be made integral, where K is the unique subfield of $\mathbb{Q}(\zeta_{57})$ of degree 12.

Integral representations

Theorem (Serre) *Let* $G = Q_8$, $K = \mathbb{Q}(\sqrt{-d})$, *and* $d > 0$. *Then*
1) G is realizable over K, $\rho : G \to GL_2(K)$, *if and only if* $d = a^2 + b^2 + c^2$ *for some integers* a, b, c.
2) G is realizable over O_K, $\rho : G \to GL_2(O_K)$, *if and only if* $d = a^2 + b^2$ *for some integers* a, b *or* $d = a^2 + 2b^2$ *for some integers* a, b.

Let G be a finite group and χ its complex irreducible character. A number field $K/\mathbb{Q}$ is called a splitting field of χ, if there exists a representation of G over K affording χ .

A splitting field K is called (degree-)minimal, if there is no splitting field of χ with degree smaller than K.

A splitting field K of χ is called integral, if any representation of G over K affording χ can be made integral. Otherwise, the splitting field K is called nonintegral.

Integral representations

Theorem (Serre) *Let $G = Q_8$, $K = \mathbb{Q}(\sqrt{-d})$, and $d > 0$. Then*
1) G is realizable over K, $\rho : G \to GL_2(K)$, if and only if $d = a^2 + b^2 + c^2$ for some integers a, b, c.
2) G is realizable over O_K, $\rho : G \to GL_2(O_K)$, if and only if $d = a^2 + b^2$ for some integers a, b or $d = a^2 + 2b^2$ for some integers a, b.

Let G be a finite group and χ its complex irreducible character. A number field $K/\mathbb{Q}$ is called a splitting field of χ, if there exists a representation of G over K affording χ .

A splitting field K is called (degree-)minimal, if there is no splitting field of χ with degree smaller than K.

A splitting field K of χ is called integral, if any representation of G over K affording χ can be made integral. Otherwise, the splitting field K is called nonintegral.

Integral representations

Let χ be an irreducible complex character of a finite group. All minimal splitting fields of χ have the same relative degree over the character field $\mathbb{Q}(\chi)$, which is called the Schur index of χ over $\mathbb{Q}$.

Notation: $m_{\mathbb{Q}(\chi)}(\chi)$.

For each place v of $\mathbb{Q}(\chi)$, there is an associated local Schur index of χ at v, denoted by $m_{\mathbb{Q}(\chi)_v}(\chi)$, and

$$m_{\mathbb{Q}(\chi)}(\chi) = LCM_v\{m_{\mathbb{Q}(\chi)_v}(\chi).\}$$

The field $\mathbb{Q}(\chi) \subset K$ is a splitting field of χ if and only if $m_{\mathbb{Q}(\chi)_v}(\chi)$ divides $[K_w : \mathbb{Q}(\chi)_v]$ for all places v of $\mathbb{Q}(\chi)$ and all divisors w of v.

Integral representations

If $m_{\mathbb{Q}}(\chi) > 1$, then there are infinitely many minimal splitting fields of χ, and if $m_{\mathbb{Q}}(\chi) = 1$, then the field of characters $\mathbb{Q}(\chi)$ is the unique minimal splitting field of χ.
Do there exist integral and nonintegral minimal splitting fields of a given character? If so, how many are there?

Let us consider the case of trivial Schur index. In this case $\mathbb{Q}(\chi)$ is the only minimal splitting field of χ. The example above shows that it can be nonintegral. On the other hand, for a character χ with $\mathbb{Q}(\chi) = \mathbb{Q}$ the minimal splitting field of χ is integral. Thus in general both cases will occur. We will now concentrate on the case $m_{\mathbb{Q}}(\chi) > 1$, more precisely on the case $m_{\mathbb{Q}}(\chi) > 1, \mathbb{Q}(\chi) = \mathbb{Q}$ and $deg(\chi) = 2$.

Theorem.

Let χ be an irreducible character of a finite group with $m_{\mathbb{Q}}(\chi) > 1, \mathbb{Q}(\chi) = \mathbb{Q}$ and $deg(\chi) = 2$. Then there exist infinitely many integral minimal splitting fields of χ, and there is infinitely many nonintegral minimal splitting fields of χ.

Remark. *This theorem holds in a more general settings, we have can find minimal integral and nonintegral splitting fields for a large number of characters of various groups assuming that χ is an irreducible character of G with $m_{\mathbb{Q}}(\chi) > 1$.*

Some related problems

The concept of global irreducibility for arithmetic rings was introduced by F. Van Oystaeyen and A.E. Zalesskii: a finite group $G \subset GL_n(F)$ over an algebraic number field F is globally irreducible if for every non-archimedean valuation v of F a Brauer reduction reduction of G (mod v) is absolutely irreducible.

Theorem (F. Van Oystaeyen and A.E. Zalesskii). O_F-span $O_F G$ of a group $G \subset GL_n(O_F)$ is equal to $M_n(O_F)$ if and only if $G \subset GL_n(O_F)$ is globally irreducible.

Problem. Describe the possible n and arithmetic rings O_F such that there is a globally irreducible $G \subset GL_n(O_F)$. What happens for $n = 2$?

n=2

Theorem. *1) Let $G = Q_{4m}$ be the group of generalized quaternions, and let $H = G = Q_8$ be the group of quaternions. Then there is a quadratic subfield $K_1 \subset K$ and an $O_{K_1}H$-module I which is an ideal in an extended field $L_1 = K_1(i)$, such that: $G = Q_{4m}$ is realizable over O_K if and only if H is realizable over O_{K_1}, and all Hilbert symbols $\left(\frac{-d, N_{L_1/\mathbb{Q}}(I)}{p}\right) = 1$ for all $p|d$.*
2) If $G = Q_{4m}$ is not realizable over O_K, the minimal realization field such that H is realizable over its ring of integers is a biquadratic extension $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, where $d = d_1 d_2$ and d_1, d_2 are integers not equal to ± 1 or to $\pm d$.
3) The explicit computation of I in $L_1 = K_1(i)$ is relevant to a representation of the integer $d = a^2 + b^2 + c^2$. N_{L_1/K_1} of either of these ideals is a principal ideal in O_{K_1} if:
(1) *$b = c$; then $d = a^2 + 2b^2$ $((a, b) = 1)$ – equivalently, d has no prime factors $p \equiv 5 (\mathrm{mod} 8)$ and $p \equiv 7 (\mathrm{mod} 8)$*, or
(2) *$c = 0$; then $d = a^2 + b^2$ $((a, b) = 1)$ or equivalently, d has no prime factors $p \equiv 3 (\mathrm{mod} 4)$.*

Some related problems

Let $\rho : G \to GL_n(\mathbb{C})$ be a complex n-dimensional representation of a finite group G. Let τ be an automorphism of the field $\mathbb{C}$, not necessarily continuous. For $g \in G$, we act by τ on the matrix coefficients of $\rho(g)$ and obtain a new matrix $\tau(\rho(g))$.

We obtain a new subgroup $\tau(\rho(G))$ in $GL_n(\mathbb{C})$. Is it possible that the subgroup $\tau(\rho(G))$ is not conjugate to $\rho(G)$ in $GL_n(\mathbb{C})$, i.e. there is no matrix $X \in GL_n(\mathbb{C})$ such that $\tau(\rho(G)) = X\rho(G)X^{-1}$?

Classification of primitive representations of Galois Groups

Classification of absolutely irreducible primitive representations of the absolute Galois groups of local fields.

Theorem. G – a finite group, H – its normal p-subgroup, G/H supersolvable, $\rho : G \to GL_n(K)$ – faithful primitive. Then:

- $n = p^d$ The center $Z = Z(H)$ is cyclic of order p^z, and for $c \in Z$ of order p there are elements $u_1, v_1, \ldots, u_d, v_d$ which together with Z generate H and satisfy the generating relations: $[u_i, u_j] = [v_i, v_j] = 1$, $[u_i, v_j] = c^{\delta_{i,j}}$, $(i, j = 1, \ldots, d)$, and the generators from different pairs commute.
- There are 2 possibilities:
  1) $u^p = v^p = 1$ for $p \neq 2$
  2) $u^p = v^p = c$ (quaternion type), or $u^p = v^p = 1$ (dihedral type) for $p = 2$.
- H/Z is p-elementary abelian of order p^{2d}
- H has $(p-1)p^{z-1}$ inequivalent faithful irr. representations

Università degli Studi di Firenze

Group Theory in Florence II

A meeting in honour of Guido Zappa

5th–7th September 2018

Invited speakers

C. Bleak (St Andrews)

J. Gonzalez (Bilbao)

M. Kassabov (Cornell)

R. Kessar (London)

M. Linckelmann (London)

A. Lucchini (Padova)

E. Pacifici (Milano)

Organising committee

Carlo Casolo, Silvio Dolfi, Francesco Fumagalli,
Eugenio Giannelli, Orazio Puglisi, Lucia Sanus

Location: viale Morgagni 67/A, Firenze, ITALY

Info at: `https://groupsinflorence2.wordpress.com/`

Università degli Studi Firenze
DIMAI
Dipartimento di Matematica e Informatica "Ulisse Dini"

INdAM
GNSAGA