Rings generated by character values of representations of finite groups

Dmitry Malinin

Università degli Studi di Padova

ISCHIA GROUP THEORY 2022

Though the traces of $g \in G$ are always algebraic integers, the representations $G \to GL_n(K)$ are not always realizable in the rings of integers O_K of algebraic number fields K.
B. Fein, B. Gordon: which fields can be generated by adjoining the entries of character tables? They proved that every Abelian extension of $\mathbb{Q}$ has a primitive element which is an entry of the character table of some finite group. They also observed a similar question for the fields generated over $\mathbb{Q}$ by one row or one column of the character table of a finite group.

Theorem (B. Fein, B. Gordon). *Let K be an Abelian extension of $\mathbb{Q}$. Then there exists a group $G = \{x_1, \ldots, x_n\}$ whose irreducible complex characters are $\chi_1, \ldots, \chi_h$, and such that*
(i) $K = \mathbb{Q}(\chi_1(x_1), \chi_1(x_2), \ldots, \chi_1(x_n))$.
(ii) $K = \mathbb{Q}(\chi_1(x_1), \chi_2(x_1), \ldots, \chi_h(x_1))$.

Representations over the field of Rationals

Gabriel Navarro and Pham Huu Tiep (2021) considered a deep problem in representation theory: for a given prime p, what is the set of abelian extensions $L_p = \{\mathbb{Q}(\chi)/\mathbb{Q} : \chi \in Irr_{p'}(G)\}$, G is a finite group?

p=2:

Theorem A1. Suppose that $\chi \in Irr(G)$ has odd degree and conductor $2^a m$, where m is odd and a is a positive integer. Then $\mathbb{Q}_{2^a} \subset \mathbb{Q}(\chi)$.

Theorem A2. Let $F/\mathbb{Q}$ be an abelian extension of $\mathbb{Q}$ with conductor $n = 2^a m$, where m is odd and a is a positive integer. Suppose that $\mathbb{Q}_{2^a} \subset F$. Then there exist a finite group G and $\chi \in Irr_{2'}(G)$ such that $F = \mathbb{Q}(\chi)$.

Integral representations

For $\chi \in Irr(G)$ and $G \subset GL_n(\mathbb{C})$ let $K_G = \mathbb{Q}(\chi(G)) = \mathbb{Q}(\{\chi(g), g \in G\})$ be the field generated by all traces of matrices in the representation of G over $\mathbb{Q}$.

We define the order generated by the character values of $\chi(G)$ over $\mathbb{Z}$ for the fixed character χ : this order $\mathbb{Z}[G]$ is contained in O_{K_G}. (Note that $\mathbb{Z}[G]$ is neither the group algebra nor the ring of generalized characters).
The deviation of $O_{K_G}[G]$ from $\mathbb{Z}[G]$ can be measured by the structure of the finite abelian group $O_{K_G}/\mathbb{Z}[G]$.

Integral representations

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.

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.

Proposition 1.
For the globally irreducible subgroups $G \subset GL_2(\mathbb{C})$ the ring of integers of $\mathbb{Q}(\chi(G))$ is $\mathbb{Z}[\chi(G)]$.

Now let $K = \mathbb{Q}(G) = \mathbb{Q}(\chi(g) : \chi \in Irr(G), g \in G)$

Proposition 2. Let G be a finite group and $K = \mathbb{Q}(G)$. Then the prime divisors of $|O_K/\mathbb{Z}[G]|$ divide $|G|$.

Proposition 3. Let $G \neq 1$ be a nilpotent group and $K = \mathbb{Q}(G)$. Then the exponent of $O_K/\mathbb{Z}[G]$ is a proper divisor of $|G|$. In particular, $|G|O_K \subset \mathbb{Z}[G]$.

Proposition 4.
1. Let $G = PSL(2, q)$ for some prime power $q \neq 1$. Then $\mathbb{O}_{\mathbb{Q}(G)} = \mathbb{Z}[G]$.

2. Let $G = Sz(q)$ for $q \geq 8$ an odd power of 2. Then $\mathbb{O}_{\mathbb{Q}(G)}/\mathbb{Z}[G]$ is isomorphic to C_2^a, where $a = \phi((q^2 + 1)(q - 1))/32$.

Integral representations and characters

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

Consider the case $deg(\chi) = 2$. 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. In general both cases will occur. We will now concentrate on the case $m_{\mathbb{Q}}(\chi) > 1$, more precisely on the case $m_{\mathbb{Q}}(\chi) > 1, \mathbb{Q}(\chi) = \mathbb{Q}$.

Integral representations and characters

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 $m_{\mathbb{Q}}(\chi) > 1$.*