Building Characters and Representations for Finite Groups

Using MAGMA

Andrea Previtali

Department of Physics and Mathematics
University of Insubria-Como, Italy

Sydney, 29 November 2007

Representations and Characters

Definitions

- Given a group G, a field F, an integer d
- we call $X \in \hom(G, \mathrm{GL}_d(F))$ a linear representation of G over F
- we assume G finite (otherwise no X might exist)
- d is called the degree of X

Definitions

- Given a group G, a field F, an integer d
- we call $X \in \hom(G, \mathrm{GL}_d(F))$ a linear representation of G over F
- we assume G finite (otherwise no X might exist)
- d is called the degree of X

Definitions

- Given a group G, a field F, an integer d
- we call $X \in \hom(G, \mathrm{GL}_d(F))$ a linear representation of G over F
- we assume G finite (otherwise no X might exist)
- d is called the degree of X

Definitions

- Given a group G, a field F, an integer d
- we call $X \in \hom(G, \mathrm{GL}_d(F))$ a linear representation of G over F
- we assume G finite (otherwise no X might exist)
- d is called the degree of X

Examples

- $1(g) = 1 \in \mathrm{GL}_1(F)$ is called the trivial representation
- if $G \leq \mathrm{GL}_d(F)$, then det is a representation of degree 1
- let Ω be a G-set, $V = \bigoplus_{\omega \in \Omega} F\omega$, δ the Kronecker's function, then $X(g)_{\alpha\beta} := \delta_{\alpha g, \beta}$ defines a representation of degree $d = |\Omega|$ over any field.
- Since $X(g)$ is a permutation matrix, X is called a permutation representation

Examples

- $1(g) = 1 \in \mathrm{GL}_1(F)$ is called the trivial representation
- if $G \leq \mathrm{GL}_d(F)$, then det is a representation of degree 1
- let Ω be a G-set, $V = \bigoplus_{\omega\in\Omega} F\omega$, δ the Kronecker's function, then $X(g)_{\alpha\beta} := \delta_{\alpha g,\beta}$ defines a representation of degree $d = |\Omega|$ over any field.
- Since $X(g)$ is a permutation matrix, X is called a permutation representation

Examples

- $1(g) = 1 \in \mathrm{GL}_1(F)$ is called the trivial representation
- if $G \leq \mathrm{GL}_d(F)$, then det is a representation of degree 1
- let Ω be a G-set, $V = \bigoplus_{\omega\in\Omega} F\omega$, δ the Kronecker's function, then $X(g)_{\alpha\beta} := \delta_{\alpha g,\beta}$ defines a representation of degree $d = |\Omega|$ over any field.
- Since $X(g)$ is a permutation matrix, X is called a permutation representation

Examples

- $1(g) = 1 \in \mathrm{GL}_1(F)$ is called the trivial representation
- if $G \leq \mathrm{GL}_d(F)$, then det is a representation of degree 1
- let Ω be a G-set, $V = \bigoplus_{\omega\in\Omega} F\omega$, δ the Kronecker's function, then $X(g)_{\alpha\beta} := \delta_{\alpha g,\beta}$ defines a representation of degree $d = |\Omega|$ over any field.
- Since $X(g)$ is a permutation matrix, X is called a permutation representation

Examples

- **Theorem (Cayley 1854)**

  Let $\Omega = G$ *via right multiplication. Then* $X(g)_{hk} = \delta_{hg,k}$ *defines* $X \in \hom(G, \mathrm{Sym}(X)) \subseteq \hom(G, GL_d(F))$

  X is called the regular representation

- $G = \mathrm{Sym}_2$, then $X((1,2)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Examples

- **Theorem (Cayley 1854)**

  Let $\Omega = G$ via right multiplication. Then $X(g)_{hk} = \delta_{hg,k}$ defines $X \in \hom(G, \mathrm{Sym}(X)) \subseteq \hom(G, GL_d(F))$

  X is called the regular representation

- $G = \mathrm{Sym}_2$, then $X((1,2)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Examples

- **Theorem (Cayley 1854)**

  Let $\Omega = G$ via right multiplication. Then $X(g)_{hk} = \delta_{hg,k}$ defines $X \in \mathrm{hom}(G, \mathrm{Sym}(X)) \subseteq \mathrm{hom}(G, GL_d(F))$

  X is called the regular representation

- $G = \mathrm{Sym}_2$, then $X((1,2)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Indecomposable

- Give $X \in \hom(G, \mathrm{GL}_d(F))$ is equivalent to define an action of G on the vector space $V = F^d$, simply via $v \cdot g = vX(g)$
  Drive on the left but act on the right!
  V is called a G-module
- a G-module V is indecomposable if $V = U \oplus W$ for G-submodules U, W implies U or $W = 0$
- a G-module V is irreducible if V has no non-trivial submodules (different from 0 or V)
- Irreducible implies indecomposable

Indecomposable

- Give $X \in \hom(G, \mathrm{GL}_d(F))$ is equivalent to define an action of G on the vector space $V = F^d$, simply via $v \cdot g = vX(g)$
  Drive on the left but act on the right!
  V is called a G-module
- a G-module V is indecomposable if $V = U \oplus W$ for G-submodules U, W implies U or $W = 0$
- a G-module V is irreducible if V has no non-trivial submodules (different from 0 or V)
- Irreducible implies indecomposable

Indecomposable

- Give $X \in \hom(G, \mathrm{GL}_d(F))$ is equivalent to define an action of G on the vector space $V = F^d$, simply via $v \cdot g = vX(g)$
  Drive on the left but act on the right!
  V is called a G-module
- a G-module V is indecomposable if $V = U \oplus W$ for G-submodules U, W implies U or $W = 0$
- a G-module V is irreducible if V has no non-trivial submodules (different from 0 or V)
- Irreducible implies indecomposable

Indecomposable

- Give $X \in \hom(G, \mathrm{GL}_d(F))$ is equivalent to define an action of G on the vector space $V = F^d$, simply via $v \cdot g = vX(g)$
  Drive on the left but act on the right!
  V is called a G-module
- a G-module V is indecomposable if $V = U \oplus W$ for G-submodules U, W implies U or $W = 0$
- a G-module V is irreducible if V has no non-trivial submodules (different from 0 or V)
- Irreducible implies indecomposable

Complete reducibility

- If $G = \mathbb{G}_a = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in F \right\}$, then $V = F^2$ is indecomposable but not irreducible
- We say a G-module V is completely reducible if $V = \bigoplus W_i$, W_i irreducible
- **Theorem (Maschke 1899)**

  If $|G| \neq 0$ in F then any finite-dimensional FG-module is completely reducible

  In particular, indecomposable=irreducible

Complete reducibility

- If $G = \mathbb{G}_a = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in F \right\}$, then $V = F^2$ is indecomposable but not irreducible
- We say a G-module V is completely reducible if $V = \bigoplus W_i$, W_i irreducible
- Theorem (Maschke 1899)

  If $|G| \neq 0$ in F then any finite-dimensional FG-module is completely reducible

  In particular, indecomposable=irreducible

Complete reducibility

- If $G = \mathbb{G}_a = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in F \right\}$, then $V = F^2$ is indecomposable but not irreducible
- We say a G-module V is completely reducible if $V = \bigoplus W_i$, W_i irreducible
- **Theorem (Maschke 1899)**

  If $|G| \neq 0$ in F then any finite-dimensional FG-module is completely reducible

  In particular, indecomposable=irreducible

Complete reducibility

- If $G = \mathbb{G}_a = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in F \right\}$, then $V = F^2$ is indecomposable but not irreducible
- We say a G-module V is completely reducible if $V = \bigoplus W_i$, W_i irreducible

- **Theorem (Maschke 1899)**

  If $|G| \neq 0$ in F then any finite-dimensional FG-module is completely reducible

  In particular, indecomposable=irreducible

Examples

- If $G = \mathrm{Sym}_2$, then the regular module V over any field F, char $F \neq 2$ splits as $T \oplus S$, where $tg = t$ and $sg = \mathrm{sgn}(g)s$
- the regular module V for any finite group G over $\mathbb{C}$ (huge field) splits as $V = \bigoplus_{i=1}^{k} d_i W_i$, where W_i are irreducible pairwise non-isomorphic

Examples

- If $G = \mathrm{Sym}_2$, then the regular module V over any field F, char $F \neq 2$ splits as $T \oplus S$, where $tg = t$ and $sg = \mathrm{sgn}(g)s$
- the regular module V for any finite group G over $\mathbb{C}$ (huge field) splits as $V = \bigoplus_{i=1}^{k} d_i W_i$, where W_i are irreducible pairwise non-isomorphic

Miracles

- Miracle 1: the number of copies d_i of any W_i equals its dimension
- Miracle 2: $k = k(G)$ the Klassenanzahl, that is, the number of conjugacy classes of G
- Miracle 3: any irreducible G-module is isomorphic to some W_i

Miracles

- Miracle 1: the number of copies d_i of any W_i equals its dimension
- Miracle 2: $k = k(G)$ the Klassenanzahl, that is, the number of conjugacy classes of G
- Miracle 3: any irreducible G-module is isomorphic to some W_i

Miracles

- Miracle 1: the number of copies d_i of any W_i equals its dimension
- Miracle 2: $k = k(G)$ the Klassenanzahl, that is, the number of conjugacy classes of G
- Miracle 3: any irreducible G-module is isomorphic to some W_i

Equivalence

- Given $X \in \hom(G, \mathrm{GL}_d(F))$, $T \in \mathrm{GL}_d(F)$), we get $Y(g) := T^{-1}X(g)T$
- X and Y are called equivalent $X \sim Y$
- if $X \sim Y$, then $\operatorname{tr} X(g) = \operatorname{tr} Y(g)$
- $\chi := \operatorname{tr} X$ is the character associated to X
- equivalent representations have the same character

Equivalence

- Given $X \in \hom(G, \mathrm{GL}_d(F))$, $T \in \mathrm{GL}_d(F))$, we get $Y(g) := T^{-1}X(g)T$
- X and Y are called equivalent $X \sim Y$
- if $X \sim Y$, then $\operatorname{tr} X(g) = \operatorname{tr} Y(g)$
- $\chi := \operatorname{tr} X$ is the character associated to X
- equivalent representations have the same character

Equivalence

- Given $X \in \hom(G, \mathrm{GL}_d(F))$, $T \in \mathrm{GL}_d(F))$, we get $Y(g) := T^{-1}X(g)T$
- X and Y are called equivalent $X \sim Y$
- if $X \sim Y$, then $\operatorname{tr} X(g) = \operatorname{tr} Y(g)$
- $\chi := \operatorname{tr} X$ is the character associated to X
- equivalent representations have the same character

Equivalence

- Given $X \in \hom(G, \mathrm{GL}_d(F))$, $T \in \mathrm{GL}_d(F))$, we get $Y(g) := T^{-1}X(g)T$
- X and Y are called equivalent $X \sim Y$
- if $X \sim Y$, then $\operatorname{tr} X(g) = \operatorname{tr} Y(g)$
- $\chi := \operatorname{tr} X$ is the character associated to X
- equivalent representations have the same character

Equivalence

- Given $X \in \hom(G, \mathrm{GL}_d(F))$, $T \in \mathrm{GL}_d(F)$), we get $Y(g) := T^{-1}X(g)T$
- X and Y are called equivalent $X \sim Y$
- if $X \sim Y$, then $\operatorname{tr} X(g) = \operatorname{tr} Y(g)$
- $\chi := \operatorname{tr} X$ is the character associated to X
- equivalent representations have the same character

More Miracles

- Miracle 3: Over $\mathbb{C}$ $X \sim Y$ iff $\operatorname{tr} X = \operatorname{tr} Y$
- so it makes sense to determine X up to equivalence given its character χ

More Miracles

- Miracle 3: Over $\mathbb{C}$ $X \sim Y$ iff $\operatorname{tr} X = \operatorname{tr} Y$
- so it makes sense to determine X up to equivalence given its character χ

Group Algebra

- **Theorem (Wedderburn 1909)**

  Let $A = \mathbb{C}G$ be the complex group algebra of G, then $A \simeq \bigoplus_{i=1}^{k} (\mathbb{C})_{d_i}$.

  - A is semisimple, that is, sum of simple algebras
  - the simple summands are full matrix algebras $(\mathbb{C})_{d_i}$ of degree d_i
  - there exists $T \in \mathrm{GL}_{|G|}(\mathbb{C})$ such that

$$R(g)^T = \mathrm{diag}(\overbrace{X_1(g), \ldots, X_1(g)}^{d_1}, \ldots, \underbrace{X_k(g), \ldots, X_k(g)}_{d_k})$$

Group Algebra

- **Theorem (Wedderburn 1909)**

  Let $A = \mathbb{C}G$ be the complex group algebra of G, then $A \simeq \bigoplus_{i=1}^{k} (\mathbb{C})_{d_i}$.

  - A is semisimple, that is, sum of simple algebras
  - the simple summands are full matrix algebras $(\mathbb{C})_{d_i}$ of degree d_i
  - there exists $T \in \mathrm{GL}_{|G|}(\mathbb{C})$ such that

$$R(g)^T = \mathrm{diag}(\overbrace{X_1(g), \ldots, X_1(g)}^{d_1}, \ldots, \underbrace{X_k(g), \ldots, X_k(g)}_{d_k})$$

Group Algebra

- **Theorem (Wedderburn 1909)**

  Let $A = \mathbb{C}G$ be the complex group algebra of G, then $A \simeq \bigoplus_{i=1}^{k} (\mathbb{C})_{d_i}$.

  - A is semisimple, that is, sum of simple algebras
  - the simple summands are full matrix algebras $(\mathbb{C})_{d_i}$ of degree d_i
  - there exists $T \in \mathrm{GL}_{|G|}(\mathbb{C})$ such that

$$R(g)^T = \mathrm{diag}(\overbrace{X_1(g), \ldots, X_1(g)}^{d_1}, \ldots, \underbrace{X_k(g), \ldots, X_k(g)}_{d_k})$$

Group Algebra

- **Theorem (Wedderburn 1909)**

  Let $A = \mathbb{C}G$ be the complex group algebra of G, then $A \simeq \bigoplus_{i=1}^{k} (\mathbb{C})_{d_i}$.

  - A is semisimple, that is, sum of simple algebras
  - the simple summands are full matrix algebras $(\mathbb{C})_{d_i}$ of degree d_i
  - there exists $T \in \mathrm{GL}_{|G|}(\mathbb{C})$ such that

$$R(g)^T = \mathrm{diag}(\overbrace{X_1(g), \dots, X_1(g)}^{d_1}, \dots, \underbrace{X_k(g), \dots, X_k(g)}_{d_k})$$

Group Algebra

- **Theorem (Wedderburn 1909)**

  Let $A = \mathbb{C}G$ be the complex group algebra of G, then $A \simeq \bigoplus_{i=1}^{k} (\mathbb{C})_{d_i}$.

  - A is semisimple, that is, sum of simple algebras
  - the simple summands are full matrix algebras $(\mathbb{C})_{d_i}$ of degree d_i
  - there exists $T \in \mathrm{GL}_{|G|}(\mathbb{C})$ such that

$$R(g)^T = \mathrm{diag}(\overbrace{X_1(g), \ldots, X_1(g)}^{d_1}, \ldots, \underbrace{X_k(g), \ldots, X_k(g)}_{d_k})$$

Center

- The center $Z := Z(\mathbb{C}G)$ is generated as a $\mathbb{C}$-vector space by $\hat{g} = \sum_{h \in g^G} h$, the sum of conjugates of g
- $\hat{g}_i \hat{g}_j = \sum_\ell c_{ij}^\ell \hat{g}_\ell$, for some integers structure constants c_{ij}^ℓ
- **Theorem (Burnside 1905, Dixon 1967, Schneider 1990)**

  Let $\chi_i = \operatorname{tr} X_i$ and $M_j = (c_{ij}^\ell)$. Then $\left(\frac{|g_\ell^G|\chi_i(g_\ell)}{\chi_i(1)}\right)_\ell$ is a common eigenvector for all M_j

Center

- The center $Z := Z(\mathbb{C}G)$ is generated as a $\mathbb{C}$-vector space by $\hat{g} = \sum_{h \in g^G} h$, the sum of conjugates of g
- $\hat{g}_i \hat{g}_j = \sum_\ell c_{ij}^\ell \hat{g}_\ell$, for some integers structure constants c_{ij}^ℓ
- **Theorem (Burnside 1905, Dixon 1967, Schneider 1990)**

  Let $\chi_i = \operatorname{tr} X_i$ and $M_j = (c_{ij}^\ell)$. Then $\left(\frac{|g_\ell^G|\chi_i(g_\ell)}{\chi_i(1)}\right)_\ell$ is a common eigenvector for all M_j

Center

- The center $Z := Z(\mathbb{C}G)$ is generated as a $\mathbb{C}$-vector space by $\hat{g} = \sum_{h \in g^G} h$, the sum of conjugates of g
- $\hat{g}_i \hat{g}_j = \sum_\ell c_{ij}^\ell \hat{g}_\ell$, for some integers structure constants c_{ij}^ℓ

- **Theorem (Burnside 1905, Dixon 1967, Schneider 1990)**

  Let $\chi_i = \operatorname{tr} X_i$ and $M_j = (c_{ij}^\ell)$. Then $\left(\frac{|g_\ell^G| \chi_i(g_\ell)}{\chi_i(1)}\right)_\ell$ is a common eigenvector for all M_j

Center

- The center $Z := Z(\mathbb{C}G)$ is generated as a $\mathbb{C}$-vector space by $\hat{g} = \sum_{h \in g^G} h$, the sum of conjugates of g
- $\hat{g}_i \hat{g}_j = \sum_\ell c_{ij}^\ell \hat{g}_\ell$, for some integers structure constants c_{ij}^ℓ

- **Theorem (Burnside 1905, Dixon 1967, Schneider 1990)**

  Let $\chi_i = \operatorname{tr} X_i$ and $M_j = (c_{ij}^\ell)$. Then $\left(\frac{|g_\ell^G| \chi_i(g_\ell)}{\chi_i(1)}\right)_\ell$ is a common eigenvector for all M_j

Approximation

- Approximation of eigenvectors
- Dixon's modular approach
- Right-Left eigenvectors

Approximation

- Approximation of eigenvectors
- Dixon's modular approach
- Right-Left eigenvectors

Approximation

- Approximation of eigenvectors
- Dixon's modular approach
- Right-Left eigenvectors

New algorithms

- Unger in 2004 found a new method to calculate the character table $T = (\chi_i(g_j))_{i,j=1}^{k}$ of a group G based on Brauer's characterization of characters and Lattice reduction techniques (LLL and PSLQ?)
- Michler and Weller in 2003 found a procedure to split permutation characters into irreducible constituents
- I extended it to monomial characters and made it efficient using a modular à la Dixon' s approach

New algorithms

- Unger in 2004 found a new method to calculate the character table $T = (\chi_i(g_j))_{i,j=1}^k$ of a group G based on Brauer's characterization of characters and Lattice reduction techniques (LLL and PSLQ?)
- Michler and Weller in 2003 found a procedure to split permutation characters into irreducible constituents
- I extended it to monomial characters and made it efficient using a modular à la Dixon' s approach

New algorithms

- Unger in 2004 found a new method to calculate the character table $T = (\chi_i(g_j))_{i,j=1}^{k}$ of a group G based on Brauer's characterization of characters and Lattice reduction techniques (LLL and PSLQ?)
- Michler and Weller in 2003 found a procedure to split permutation characters into irreducible constituents
- I extended it to monomial characters and made it efficient using a modular à la Dixon' s approach

MeatAxe

- A a finite-dimensional algebra over a finite field F, e.g. $A = FG$, and V an A-module
- establish whether V is irreducible and if not find a proper submodule W
- Parker 1984: Choose a random element a in A hope it has small non-zero nullity, pick $w \in \ker a$ and hope that $W := wA$ is a proper submodule of V. In this case we call a a splitting element
- Norton's irreducibility criterion

MeatAxe

- A a finite-dimensional algebra over a finite field F, e.g. $A = FG$, and V an A-module
- establish whether V is irreducible and if not find a proper submodule W
- Parker 1984: Choose a random element a in A hope it has small non-zero nullity, pick $w \in \ker a$ and hope that $W := wA$ is a proper submodule of V. In this case we call a a splitting element
- Norton's irreducibility criterion

MeatAxe

- A a finite-dimensional algebra over a finite field F, e.g. $A = FG$, and V an A-module
- establish whether V is irreducible and if not find a proper submodule W
- Parker 1984: Choose a random element a in A hope it has small non-zero nullity, pick $w \in \ker a$ and hope that $W := wA$ is a proper submodule of V. In this case we call a a splitting element
- Norton's irreducibility criterion

MeatAxe

- A a finite-dimensional algebra over a finite field F, e.g. $A = FG$, and V an A-module
- establish whether V is irreducible and if not find a proper submodule W
- Parker 1984: Choose a random element a in A hope it has small non-zero nullity, pick $w \in \ker a$ and hope that $W := wA$ is a proper submodule of V. In this case we call a a splitting element
- Norton's irreducibility criterion

MeatAxe

- Holt and Rees 1994: Choose random $b \in A$, calculate its minimal polynomial $m(x)$ and an irreducible factor $p(x)$, use $a := p(b)$
- high probability unless V reducible, $V/Rad(V)$ irreducible but not absolutely irreducible, all composition factors are isomorphic
- Ivanyos-Lux 2000: Solution of the exceptional case

MeatAxe

- Holt and Rees 1994: Choose random $b \in A$, calculate its minimal polynomial $m(x)$ and an irreducible factor $p(x)$, use $a := p(b)$
- high probability unless V reducible, $V/Rad(V)$ irreducible but not absolutely irreducible, all composition factors are isomorphic
- Ivanyos-Lux 2000: Solution of the exceptional case

MeatAxe

- Holt and Rees 1994: Choose random $b \in A$, calculate its minimal polynomial $m(x)$ and an irreducible factor $p(x)$, use $a := p(b)$
- high probability unless V reducible, $V/Rad(V)$ irreducible but not absolutely irreducible, all composition factors are isomorphic
- Ivanyos-Lux 2000: Solution of the exceptional case

Tensor Products

- Given two representations X, Y of a group G we may form a new one T as tensor product

- **Theorem (Burnside 1911, Brauer 1964)**

  Let X be a faithful representation of group G then any irreducible representation Y of G occurs as a composition factor of some tensor power $X^{\otimes n}$ of X

  - When char(F) does not divide $|G|$ we have that any irreducible FG-module is a submodule of $V^{\otimes n}$, where V affords X
  - When char(F) $= 0$, one can show it suffices to consider $0 \leq n \leq m - 1$ where $m = |\{\chi(g) : g \in G\}$ and $\chi = \operatorname{tr} X$
  - For example, $m = 2$ when X is the regular representation

Tensor Products

- Given two representations X, Y of a group G we may form a new one T as tensor product
- **Theorem (Burnside 1911, Brauer 1964)**

  Let X be a faithful representation of group G then any irreducible representation Y of G occurs as a composition factor of some tensor power $X^{\otimes n}$ of X

  - When char(F) does not divide $|G|$ we have that any irreducible FG-module is a submodule of $V^{\otimes n}$, where V affords X
  - When char(F) $= 0$, one can show it suffices to consider $0 \leq n \leq m-1$ where $m = |\{\chi(g) : g \in G\}$ and $\chi = \operatorname{tr} X$
  - For example, $m = 2$ when X is the regular representation

Tensor Products

- Given two representations X, Y of a group G we may form a new one T as tensor product

- **Theorem (Burnside 1911, Brauer 1964)**

  Let X be a faithful representation of group G then any irreducible representation Y of G occurs as a composition factor of some tensor power $X^{\otimes n}$ of X

- When char(F) does not divide $|G|$ we have that any irreducible FG-module is a submodule of $V^{\otimes n}$, where V affords X
- When char$(F) = 0$, one can show it suffices to consider $0 \leq n \leq m - 1$ where $m = |\{\chi(g) : g \in G\}$ and $\chi = \text{tr}\, X$
- For example, $m = 2$ when X is the regular representation

Tensor Products

- Given two representations X, Y of a group G we may form a new one T as tensor product

- **Theorem (Burnside 1911, Brauer 1964)**

  Let X be a faithful representation of group G then any irreducible representation Y of G occurs as a composition factor of some tensor power $X^{\otimes n}$ of X

- When $\text{char}(F)$ does not divide $|G|$ we have that any irreducible FG-module is a submodule of $V^{\otimes n}$, where V affords X
- When $\text{char}(F) = 0$, one can show it suffices to consider $0 \leq n \leq m-1$ where $m = |\{\chi(g) : g \in G\}$ and $\chi = \text{tr}\, X$
- For example, $m = 2$ when X is the regular representation

Tensor Products

- Given two representations X, Y of a group G we may form a new one T as tensor product
- **Theorem (Burnside 1911, Brauer 1964)**

  Let X be a faithful representation of group G then any irreducible representation Y of G occurs as a composition factor of some tensor power $X^{\otimes n}$ of X

  - When char(F) does not divide $|G|$ we have that any irreducible FG-module is a submodule of $V^{\otimes n}$, where V affords X
  - When char$(F) = 0$, one can show it suffices to consider $0 \leq n \leq m-1$ where $m = |\{\chi(g) \,:\, g \in G\}$ and $\chi = \operatorname{tr} X$
  - For example, $m = 2$ when X is the regular representation

Tensor Products

- Given two representations X, Y of a group G we may form a new one T as tensor product

- **Theorem (Burnside 1911, Brauer 1964)**

  Let X be a faithful representation of group G then any irreducible representation Y of G occurs as a composition factor of some tensor power $X^{\otimes n}$ of X

- When char(F) does not divide $|G|$ we have that any irreducible FG-module is a submodule of $V^{\otimes n}$, where V affords X
- When char$(F) = 0$, one can show it suffices to consider $0 \leq n \leq m - 1$ where $m = |\{\chi(g) : g \in G\}$ and $\chi = \operatorname{tr} X$
- For example, $m = 2$ when X is the regular representation

Integral MeatAxe

- Extend MeatAxe to fields of characteristic 0
- Parker in 1998 suggested a procedure when $F = \mathbb{Q}$. No estimate regarding chances to hit a splitting element
- Dixon in 1970 proposes a procedure to split a given irreducible unitary representation. Given a set S of generators for a finite subgroup G of $\mathrm{U}_d(\mathbb{C})$, define

$$\sigma : b \mapsto \frac{1}{|S|} \sum_{u \in S} {}^t\bar{u} b u,$$

then $\sigma^n(b_0)$ converges to a matrix a such that $au = ua$, for all $u \in S$, hence for all $u \in G$. Eigenspaces of a allow to split G

Integral MeatAxe

- Extend MeatAxe to fields of characteristic 0
- Parker in 1998 suggested a procedure when $F = \mathbb{Q}$. No estimate regarding chances to hit a splitting element
- Dixon in 1970 proposes a procedure to split a given irreducible unitary representation. Given a set S of generators for a finite subgroup G of $\mathrm{U}_d(\mathbb{C})$, define

$$\sigma : b \mapsto \frac{1}{|S|} \sum_{u \in S} {}^t\overline{u} b u,$$

then $\sigma^n(b_0)$ converges to a matrix a such that $au = ua$, for all $u \in S$, hence for all $u \in G$. Eigenspaces of a allow to split G

Integral MeatAxe

- Extend MeatAxe to fields of characteristic 0
- Parker in 1998 suggested a procedure when $F = \mathbb{Q}$. No estimate regarding chances to hit a splitting element
- Dixon in 1970 proposes a procedure to split a given irreducible unitary representation. Given a set S of generators for a finite subgroup G of $\mathrm{U}_d(\mathbb{C})$, define

$$\sigma : b \mapsto \frac{1}{|S|} \sum_{u \in S} {}^t\overline{u} b u,$$

then $\sigma^n(b_0)$ converges to a matrix a such that $au = ua$, for all $u \in S$, hence for all $u \in G$. Eigenspaces of a allow to split G

Idempotents and splitting

- We say a is idempotent if $a^2 = a$
- Given a G-module V let $\mathrm{End}_G(V) = \{a \in \mathrm{End}(V) : ag = ga\}$
- If $|G| \neq 0 \in F$, then any G-submodule U has shape Va for some idempotent $a \in \mathrm{End}_G(V)$
- In general, $W = Va$ is a submodule for any $a \in \mathrm{End}_G(V)$

Idempotents and splitting

- We say a is idempotent if $a^2 = a$
- Given a G-module V let $\mathrm{End}_G(V) = \{a \in \mathrm{End}(V) \ : \ ag = ga\}$
- If $|G| \neq 0 \in F$, then any G-submodule U has shape Va for some idempotent $a \in \mathrm{End}_G(V)$
- In general, $W = Va$ is a submodule for any $a \in \mathrm{End}_G(V)$

Idempotents and splitting

- We say a is idempotent if $a^2 = a$
- Given a G-module V let $\mathrm{End}_G(V) = \{a \in \mathrm{End}(V) : ag = ga\}$
- If $|G| \neq 0 \in F$, then any G-submodule U has shape Va for some idempotent $a \in \mathrm{End}_G(V)$
- In general, $W = Va$ is a submodule for any $a \in \mathrm{End}_G(V)$

Idempotents and splitting

- We say a is idempotent if $a^2 = a$
- Given a G-module V let $\mathrm{End}_G(V) = \{a \in \mathrm{End}(V) \;:\; ag = ga\}$
- If $|G| \neq 0 \in F$, then any G-submodule U has shape Va for some idempotent $a \in \mathrm{End}_G(V)$
- In general, $W = Va$ is a submodule for any $a \in \mathrm{End}_G(V)$

Induction and Restriction

- Given a subgroup H and an FH-module W, construct the induced module $W\upharpoonright^G = \bigoplus_{t\in T} W \otimes t$ where $G = \bigsqcup_{t\in T} Ht$ via

$$(w \otimes t)g = wh \otimes t \cdot g,$$

where $tg = h(t \cdot g)$

- We say a representation Y of H extends to G if there exists X of G such that $X(h) = Y(h), \forall h \in H$
- Let H be a normal subgroup of prime index in G and W an irreducible FH-module, then either W extends or $W\upharpoonright^G$ is irreducible

Induction and Restriction

- Given a subgroup H and an FH-module W, construct the induced module $W\upharpoonright^G = \bigoplus_{t \in T} W \otimes t$ where $G = \bigsqcup_{t \in T} Ht$ via

$$(w \otimes t)g = wh \otimes t \cdot g,$$

where $tg = h(t \cdot g)$

- We say a representation Y of H extends to G if there exists X of G such that $X(h) = Y(h), \forall h \in H$
- Let H be a normal subgroup of prime index in G and W an irreducible FH-module, then either W extends or $W\upharpoonright^G$ is irreducible

Induction and Restriction

- Given a subgroup H and an FH-module W, construct the induced module $W\upharpoonright^G = \bigoplus_{t\in T} W \otimes t$ where $G = \bigsqcup_{t\in T} Ht$ via

$$(w \otimes t)g = wh \otimes t \cdot g,$$

where $tg = h(t \cdot g)$
- We say a representation Y of H extends to G if there exists X of G such that $X(h) = Y(h), \forall h \in H$
- Let H be a normal subgroup of prime index in G and W an irreducible FH-module, then either W extends or $W\upharpoonright^G$ is irreducible

Soluble case

- Assume G soluble, then there exist $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = 1$, with G_i/G_{i+1} of prime order
- Given $\chi \in \mathrm{Irr}(G)$ we start from $G_n = 1$ and build representations for irreducible constituents of the restriction of χ to G_i
- Glasby, Howlett 1997, Brückner 1998 implement it when F is finite and infinite respectively
- If Y representation of H extendable to $H\langle g\rangle$, then $Y(h) = T^{-1}Y^g(h)T$, for some T. Set $X(g) := \lambda T$, $X(h) := Y(h)$, for a suitable $\lambda \in F$

Soluble case

- Assume G soluble, then there exist $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = 1$, with G_i/G_{i+1} of prime order
- Given $\chi \in \mathrm{Irr}(G)$ we start from $G_n = 1$ and build representations for irreducible constituents of the restriction of χ to G_i
- Glasby, Howlett 1997, Brückner 1998 implement it when F is finite and infinite respectively
- If Y representation of H extendable to $H\langle g\rangle$, then $Y(h) = T^{-1}Y^g(h)T$, for some T. Set $X(g) := \lambda T$, $X(h) := Y(h)$, for a suitable $\lambda \in F$

Soluble case

- Assume G soluble, then there exist $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = 1$, with G_i/G_{i+1} of prime order
- Given $\chi \in \mathrm{Irr}(G)$ we start from $G_n = 1$ and build representations for irreducible constituents of the restriction of χ to G_i
- Glasby, Howlett 1997, Brückner 1998 implement it when F is finite and infinite respectively
- If Y representation of H extendable to $H\langle g\rangle$, then $Y(h) = T^{-1}Y^g(h)T$, for some T. Set $X(g) := \lambda T$, $X(h) := Y(h)$, for a suitable $\lambda \in F$

Soluble case

- Assume G soluble, then there exist $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = 1$, with G_i/G_{i+1} of prime order
- Given $\chi \in \mathrm{Irr}(G)$ we start from $G_n = 1$ and build representations for irreducible constituents of the restriction of χ to G_i
- Glasby, Howlett 1997, Brückner 1998 implement it when F is finite and infinite respectively
- If Y representation of H extendable to $H\langle g\rangle$, then $Y(h) = T^{-1}Y^g(h)T$, for some T. Set $X(g) := \lambda T$, $X(h) := Y(h)$, for a suitable $\lambda \in F$

Primitive Central Idempotents

- Given an irreducible complex character χ of G, $e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$ is a primitive central idempotent
- $e_\chi \mathbb{C}G \simeq (\mathbb{C})_d$, $d = \chi(1)$
- Purpose: Find $a \in \mathbb{C}G$ such that ae_χ has rank d. Notice this is minimum non-zero
- Then $W = Vae_\chi$ has dimension d, where V is the regular module, and affords χ

Primitive Central Idempotents

- Given an irreducible complex character χ of G, $e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$ is a primitive central idempotent
- $e_\chi \mathbb{C}G \simeq (\mathbb{C})_d$, $d = \chi(1)$
- Purpose: Find $a \in \mathbb{C}G$ such that ae_χ has rank d. Notice this is minimum non-zero
- Then $W = Vae_\chi$ has dimension d, where V is the regular module, and affords χ

Primitive Central Idempotents

- Given an irreducible complex character χ of G, $e_\chi = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g$ is a primitive central idempotent
- $e_\chi\mathbb{C}G \simeq (\mathbb{C})_d$, $d = \chi(1)$
- Purpose: Find $a \in \mathbb{C}G$ such that ae_χ has rank d. Notice this is minimum non-zero
- Then $W = Vae_\chi$ has dimension d, where V is the regular module, and affords χ

Primitive Central Idempotents

- Given an irreducible complex character χ of G, $e_\chi = \frac{\chi(1)}{|G|}\sum_{g \in G} \chi(g^{-1})g$ is a primitive central idempotent
- $e_\chi \mathbb{C}G \simeq (\mathbb{C})_d$, $d = \chi(1)$
- Purpose: Find $a \in \mathbb{C}G$ such that ae_χ has rank d. Notice this is minimum non-zero
- Then $W = Vae_\chi$ has dimension d, where V is the regular module, and affords χ

Subgroup Idempotents

- A deterministic approach: given $H \leq G$ and $\vartheta \in \mathrm{Irr}(H)$ take $a = \frac{\vartheta(1)}{|H|} \sum_{h \in H} \vartheta(h^{-1})h$, a subgroup-idempotent
- call H a χ-good subgroup if χ_H has a linear constituent with multiplicity 1

- **Theorem (Dixon 1993)**

  If G admits a χ-good subgroup, then a representation X affording χ can be constructed

Subgroup Idempotents

- A deterministic approach: given $H \leq G$ and $\vartheta \in \mathrm{Irr}(H)$ take $a = \frac{\vartheta(1)}{|H|} \sum_{h \in H} \vartheta(h^{-1})h$, a subgroup-idempotent
- call H a χ-good subgroup if χ_H has a linear constituent with multiplicity 1

- **Theorem (Dixon 1993)**

  If G admits a χ-good subgroup, then a representation X affording χ can be constructed

Subgroup Idempotents

- A deterministic approach: given $H \leq G$ and $\vartheta \in \mathrm{Irr}(H)$ take $a = \frac{\vartheta(1)}{|H|} \sum_{h \in H} \vartheta(h^{-1})h$, a subgroup-idempotent
- call H a χ-good subgroup if χ_H has a linear constituent with multiplicity 1

- **Theorem (Dixon 1993)**

  If G admits a χ-good subgroup, then a representation X affording χ can be constructed

Subgroup Idempotents

- A deterministic approach: given $H \leq G$ and $\vartheta \in \mathrm{Irr}(H)$ take $a = \frac{\vartheta(1)}{|H|} \sum_{h \in H} \vartheta(h^{-1})h$, a subgroup-idempotent
- call H a χ-good subgroup if χ_H has a linear constituent with multiplicity 1

- **Theorem (Dixon 1993)**

  If G admits a χ-good subgroup, then a representation X affording χ can be constructed

Hermitian Matrices

- Given a good subgroup constructs a hermitian matrix A of rank d indexed by elements in G
- chooses d random elements from A hoping to obtain linearly independent rows
- the principal submatrix $A(1)$ corresponding to these rows is non-singular
- obtain $X(g) = A(g)A(1)^{-1}$, where $A(g)$ is a slight variation of $A(1)$
- Glauberman-Janusz 1966 have given examples of pairs (G, χ) without good subgroups

Hermitian Matrices

- Given a good subgroup constructs a hermitian matrix A of rank d indexed by elements in G
- chooses d random elements from A hoping to obtain linearly independent rows
- the principal submatrix $A(1)$ corresponding to these rows is non-singular
- obtain $X(g) = A(g)A(1)^{-1}$, where $A(g)$ is a slight variation of $A(1)$
- Glauberman-Janusz 1966 have given examples of pairs (G, χ) without good subgroups

Hermitian Matrices

- Given a good subgroup constructs a hermitian matrix A of rank d indexed by elements in G
- chooses d random elements from A hoping to obtain linearly independent rows
- the principal submatrix $A(1)$ corresponding to these rows is non-singular
- obtain $X(g) = A(g)A(1)^{-1}$, where $A(g)$ is a slight variation of $A(1)$
- Glauberman-Janusz 1966 have given examples of pairs (G, χ) without good subgroups

Hermitian Matrices

- Given a good subgroup constructs a hermitian matrix A of rank d indexed by elements in G
- chooses d random elements from A hoping to obtain linearly independent rows
- the principal submatrix $A(1)$ corresponding to these rows is non-singular
- obtain $X(g) = A(g)A(1)^{-1}$, where $A(g)$ is a slight variation of $A(1)$
- Glauberman-Janusz 1966 have given examples of pairs (G, χ) without good subgroups

Hermitian Matrices

- Given a good subgroup constructs a hermitian matrix A of rank d indexed by elements in G
- chooses d random elements from A hoping to obtain linearly independent rows
- the principal submatrix $A(1)$ corresponding to these rows is non-singular
- obtain $X(g) = A(g)A(1)^{-1}$, where $A(g)$ is a slight variation of $A(1)$
- Glauberman-Janusz 1966 have given examples of pairs (G, χ) without good subgroups

Real Idempotents

- a group algebra FG, where $F = \overline{F}$ has more structure, namely has an involution or anti-automorphism defined as

$$* : \sum a_g g \mapsto \sum \overline{a_g} g^{-1}$$

- we say an element a of FG is real if $a^* = a$
- Notice that subgroups idempotents are real since $\chi(g^{-1}) = \overline{\chi(g)}$

Real Idempotents

- a group algebra FG, where $F = \overline{F}$ has more structure, namely has an involution or anti-automorphism defined as
$$* : \sum a_g g \mapsto \sum \overline{a_g} g^{-1}$$
- we say an element a of FG is real if $a^* = a$
- Notice that subgroups idempotents are real since $\chi(g^{-1}) = \overline{\chi(g)}$

Real Idempotents

- a group algebra FG, where $F = \overline{F}$ has more structure, namely has an involution or anti-automorphism defined as
$$* : \sum a_g g \mapsto \sum \overline{a_g} g^{-1}$$
- we say an element a of FG is real if $a^* = a$
- Notice that subgroups idempotents are real since $\chi(g^{-1}) = \overline{\chi(g)}$

Generalizing Dixon and Homogeneous Modules

- Let $m = \vartheta(1)(\chi_H, \vartheta)$ then Dixon's algorithm can be modified to yield a homogeneous module $V = mW$, where W affords χ
- V is realized over $\mathbb{Q}(\chi, \vartheta) = \mathbb{Q}(\chi(G), \vartheta(H))$
- Obstruction: MeatAxe works well if the characteristic polynomial has few repeated factors, but here they are m-th powers

Generalizing Dixon and Homogeneous Modules

- Let $m = \vartheta(1)(\chi_H, \vartheta)$ then Dixon's algorithm can be modified to yield a homogeneous module $V = mW$, where W affords χ
- V is realized over $\mathbb{Q}(\chi, \vartheta) = \mathbb{Q}(\chi(G), \vartheta(H))$
- Obstruction: MeatAxe works well if the characteristic polynomial has few repeated factors, but here they are m-th powers

Generalizing Dixon and Homogeneous Modules

- Let $m = \vartheta(1)(\chi_H, \vartheta)$ then Dixon's algorithm can be modified to yield a homogeneous module $V = mW$, where W affords χ
- V is realized over $\mathbb{Q}(\chi, \vartheta) = \mathbb{Q}(\chi(G), \vartheta(H))$
- Obstruction: MeatAxe works well if the characteristic polynomial has few repeated factors, but here they are m-th powers

Why Subgroup-Idempotents?

- We might just look for arbitrary elements $a \in FG$ such that $\mathrm{rk}(ae_\chi) = \chi(1)$
- For example nilpotent elements $a \neq a^2 = 0$
- There are many more idempotents in FG than subgroup-idempotents
- To use Dixon's approach real idempotents are needed
- Problem: are they subgroup-idempotents?

Why Subgroup-Idempotents?

- We might just look for arbitrary elements $a \in FG$ such that $\mathrm{rk}(ae_\chi) = \chi(1)$
- For example nilpotent elements $a \neq a^2 = 0$
- There are many more idempotents in FG than subgroup-idempotents
- To use Dixon's approach real idempotents are needed
- Problem: are they subgroup-idempotents?

Why Subgroup-Idempotents?

- We might just look for arbitrary elements $a \in FG$ such that $\mathrm{rk}(ae_\chi) = \chi(1)$
- For example nilpotent elements $a \neq a^2 = 0$
- There are many more idempotents in FG than subgroup-idempotents
- To use Dixon's approach real idempotents are needed
- Problem: are they subgroup-idempotents?

Why Subgroup-Idempotents?

- We might just look for arbitrary elements $a \in FG$ such that $\mathrm{rk}(ae_\chi) = \chi(1)$
- For example nilpotent elements $a \neq a^2 = 0$
- There are many more idempotents in FG than subgroup-idempotents
- To use Dixon's approach real idempotents are needed
- Problem: are they subgroup-idempotents?

Why Subgroup-Idempotents?

- We might just look for arbitrary elements $a \in FG$ such that $\mathrm{rk}(ae_\chi) = \chi(1)$
- For example nilpotent elements $a \neq a^2 = 0$
- There are many more idempotents in FG than subgroup-idempotents
- To use Dixon's approach real idempotents are needed
- Problem: are they subgroup-idempotents?

Minimal Splitting Fields

- Given a complex irreducible character χ, which is the field E of minimum degree over F realizing χ?
  $X \in \hom(G, GL_d(E))$, $\chi = \operatorname{tr} X$, $|E : F|$ minimum.
- We call E a minimal splitting field for χ

- **Theorem (Brauer 1954)**

  Let $e = \operatorname{Exp}(G)$, then $\mathbb{Q}(\xi_e)$, ξ_e a primitive e-th root of unity, is a splitting field for (any representation) of G

- Hence we can drop down from $\mathbb{C}$ to a finite-degree extension of $\mathbb{Q}$ (algebraic number field)

Minimal Splitting Fields

- Given a complex irreducible character χ, which is the field E of minimum degree over F realizing χ? $X \in \hom(G, GL_d(E))$, $\chi = \operatorname{tr} X$, $|E : F|$ minimum.
- We call E a minimal splitting field for χ
- **Theorem (Brauer 1954)**

  Let $e = \operatorname{Exp}(G)$, then $\mathbb{Q}(\xi_e)$, ξ_e a primitive e-th root of unity, is a splitting field for (any representation) of G

- Hence we can drop down from $\mathbb{C}$ to a finite-degree extension of $\mathbb{Q}$ (algebraic number field)

Minimal Splitting Fields

- Given a complex irreducible character χ, which is the field E of minimum degree over F realizing χ? $X \in \hom(G, GL_d(E))$, $\chi = \operatorname{tr} X$, $|E : F|$ minimum.
- We call E a minimal splitting field for χ

- **Theorem (Brauer 1954)**

  Let $e = \operatorname{Exp}(G)$, then $\mathbb{Q}(\xi_e)$, ξ_e a primitive e-th root of unity, is a splitting field for (any representation) of G

- Hence we can drop down from $\mathbb{C}$ to a finite-degree extension of $\mathbb{Q}$ (algebraic number field)

Minimal Splitting Fields

- Given a complex irreducible character χ, which is the field E of minimum degree over F realizing χ? $X \in \hom(G, GL_d(E))$, $\chi = \operatorname{tr} X$, $|E : F|$ minimum.
- We call E a minimal splitting field for χ
- **Theorem (Brauer 1954)**

  Let $e = \operatorname{Exp}(G)$, then $\mathbb{Q}(\xi_e)$, ξ_e a primitive e-th root of unity, is a splitting field for (any representation) of G
- Hence we can drop down from $\mathbb{C}$ to a finite-degree extension of $\mathbb{Q}$ (algebraic number field)

Minimal Splitting Fields

- Given a complex irreducible character χ, which is the field E of minimum degree over F realizing χ? $X \in \hom(G, GL_d(E))$, $\chi = \operatorname{tr} X$, $|E : F|$ minimum.
- We call E a minimal splitting field for χ

- **Theorem (Brauer 1954)**

  Let $e = \operatorname{Exp}(G)$, then $\mathbb{Q}(\xi_e)$, ξ_e a primitive e-th root of unity, is a splitting field for (any representation) of G

- Hence we can drop down from $\mathbb{C}$ to a finite-degree extension of $\mathbb{Q}$ (algebraic number field)

Character Fields

- Clearly any splitting field F for χ contains the character field $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g) \ : \ g \in G)$
- Define the Schur index $m_F(\chi)$ of χ as $|E : F(\chi)|$, E a minimal splitting field over F
- Let $f(\chi)$ be the minimum integer f such that $\mathbb{Q}(\chi) \leq \mathbb{Q}(\xi_f)$, $f(\chi)$ is called the conductor of χ

Character Fields

- Clearly any splitting field F for χ contains the character field $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g) \; : \; g \in G)$
- Define the Schur index $m_F(\chi)$ of χ as $|E : F(\chi)|$, E a minimal splitting field over F
- Let $f(\chi)$ be the minimum integer f such that $\mathbb{Q}(\chi) \leq \mathbb{Q}(\xi_f)$, $f(\chi)$ is called the conductor of χ

Character Fields

- Clearly any splitting field F for χ contains the character field $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g) \, : \, g \in G)$
- Define the Schur index $m_F(\chi)$ of χ as $|E : F(\chi)|$, E a minimal splitting field over F
- Let $f(\chi)$ be the minimum integer f such that $\mathbb{Q}(\chi) \leq \mathbb{Q}(\xi_f)$, $f(\chi)$ is called the conductor of χ

Embedding in Cyclotomic Fields

- E need not be contained in $\mathbb{Q}(\xi_e)$
- the group of quaternions $G = Q_8$ has a unique 2-dimensional irreducible character χ
- $\mathbb{Q}(\chi) = \mathbb{Q}$, so $f(\chi) = 1$ but no $X \in \hom(G, GL_2(\mathbb{Q}))$ affords χ

Embedding in Cyclotomic Fields

- E need not be contained in $\mathbb{Q}(\xi_e)$
- the group of quaternions $G = Q_8$ has a unique 2-dimensional irreducible character χ
- $\mathbb{Q}(\chi) = \mathbb{Q}$, so $f(\chi) = 1$ but no $X \in \hom(G, GL_2(\mathbb{Q}))$ affords χ

Embedding in Cyclotomic Fields

- E need not be contained in $\mathbb{Q}(\xi_e)$
- the group of quaternions $G = Q_8$ has a unique 2-dimensional irreducible character χ
- $\mathbb{Q}(\chi) = \mathbb{Q}$, so $f(\chi) = 1$ but no $X \in \mathrm{hom}(G, GL_2(\mathbb{Q}))$ affords χ

Embedding in Cyclotomic Fields II

- Lorenz 1964, Fieker, Nebe, Unger 2007 the Schur index can be calculated $m_{\mathbb{Q}}(\chi) = 2$
- there exists X over $\mathbb{Q}(\xi_5)$ affording χ
- but X can not be realized over the unique quadratic subfield of $\mathbb{Q}(\xi_5)$

Embedding in Cyclotomic Fields II

- Lorenz 1964, Fieker, Nebe, Unger 2007 the Schur index can be calculated $m_{\mathbb{Q}}(\chi) = 2$
- there exists X over $\mathbb{Q}(\xi_5)$ affording χ
- but X can not be realized over the unique quadratic subfield of $\mathbb{Q}(\xi_5)$

Embedding in Cyclotomic Fields II

- Lorenz 1964, Fieker, Nebe, Unger 2007 the Schur index can be calculated $m_{\mathbb{Q}}(\chi) = 2$
- there exists X over $\mathbb{Q}(\xi_5)$ affording χ
- but X can not be realized over the unique quadratic subfield of $\mathbb{Q}(\xi_5)$

Central Simple Algebras

- $\mathbb{Q}Q_8 \simeq 4\mathbb{Q} \oplus \mathbb{H}$, and $\mathbb{H}$ is the division ring of quaternions
- $\mathbb{H}$ is an example of central simple algebra, namely a simple algebra of finite dimension over its center
- an algebra A is said to be cyclic of degree s over F if

$$A \simeq F\langle a, b \,|\, m(a) = 0, ab = ba^{\alpha}, b^s = c\rangle$$

where $c \in F$, $m(x) \in F[x]$ irreducible, $F[a]$ is a Galois extension of F and the Galois group is generated by α

- **Theorem (Albert-Brauer-Hasse-Noether 1931)**

  Every central simple algebra over an algebraic number field is cyclic

Central Simple Algebras

- $\mathbb{Q}Q_8 \simeq 4\mathbb{Q} \oplus \mathbb{H}$, and $\mathbb{H}$ is the division ring of quaternions
- $\mathbb{H}$ is an example of central simple algebra, namely a simple algebra of finite dimension over its center
- an algebra A is said to be cyclic of degree s over F if

$$A \simeq F\langle a, b \mid m(a) = 0, ab = ba^{\alpha}, b^s = c\rangle$$

where $c \in F$, $m(x) \in F[x]$ irreducible, $F[a]$ is a Galois extension of F and the Galois group is generated by α

- **Theorem (Albert-Brauer-Hasse-Noether 1931)**

Every central simple algebra over an algebraic number field is cyclic

Central Simple Algebras

- $\mathbb{Q}Q_8 \simeq 4\mathbb{Q} \oplus \mathbb{H}$, and $\mathbb{H}$ is the division ring of quaternions
- $\mathbb{H}$ is an example of central simple algebra, namely a simple algebra of finite dimension over its center
- an algebra A is said to be cyclic of degree s over F if

$$A \simeq F\langle a, b \mid m(a) = 0, ab = ba^{\alpha}, b^s = c\rangle$$

where $c \in F$, $m(x) \in F[x]$ irreducible, $F[a]$ is a Galois extension of F and the Galois group is generated by α

- **Theorem (Albert-Brauer-Hasse-Noether 1931)**

  Every central simple algebra over an algebraic number field is cyclic

Central Simple Algebras

- $\mathbb{Q}Q_8 \simeq 4\mathbb{Q} \oplus \mathbb{H}$, and $\mathbb{H}$ is the division ring of quaternions
- $\mathbb{H}$ is an example of central simple algebra, namely a simple algebra of finite dimension over its center
- an algebra A is said to be cyclic of degree s over F if

$$A \simeq F\langle a, b \mid m(a) = 0, ab = ba^{\alpha}, b^s = c\rangle$$

where $c \in F$, $m(x) \in F[x]$ irreducible, $F[a]$ is a Galois extension of F and the Galois group is generated by α

- **Theorem (Albert-Brauer-Hasse-Noether 1931)**

  Every central simple algebra over an algebraic number field is cyclic

Central Simple Algebras

- $\mathbb{Q}Q_8 \simeq 4\mathbb{Q} \oplus \mathbb{H}$, and $\mathbb{H}$ is the division ring of quaternions
- $\mathbb{H}$ is an example of central simple algebra, namely a simple algebra of finite dimension over its center
- an algebra A is said to be cyclic of degree s over F if

$$A \simeq F\langle a, b \mid m(a) = 0, ab = ba^\alpha, b^s = c\rangle$$

where $c \in F$, $m(x) \in F[x]$ irreducible, $F[a]$ is a Galois extension of F and the Galois group is generated by α

- **Theorem (Albert-Brauer-Hasse-Noether 1931)**

  Every central simple algebra over an algebraic number field is cyclic

Wedderburn Decomposition

- for any group G, $\mathbb{Q}G \simeq \bigoplus (D_i)_{d_i}$, where D_i is a division ring
- Let $Z_i = Z(D_i)$, then $Z_i = \mathbb{Q}(\chi_i)$ for some $\chi_i \in \mathrm{Irr}(G)$
- If $t_i = |Z_i : \mathbb{Q}|$, then the t_i conjugates of χ_i are exactly those characters not annihilating $(D_i)_{d_i}$

Wedderburn Decomposition

- for any group G, $\mathbb{Q}G \simeq \bigoplus (D_i)_{d_i}$, where D_i is a division ring
- Let $Z_i = Z(D_i)$, then $Z_i = \mathbb{Q}(\chi_i)$ for some $\chi_i \in \mathrm{Irr}(G)$
- If $t_i = |Z_i : \mathbb{Q}|$, then the t_i conjugates of χ_i are exactly those characters not annihilating $(D_i)_{d_i}$

Wedderburn Decomposition

- for any group G, $\mathbb{Q}G \simeq \bigoplus (D_i)_{d_i}$, where D_i is a division ring
- Let $Z_i = Z(D_i)$, then $Z_i = \mathbb{Q}(\chi_i)$ for some $\chi_i \in \text{Irr}(G)$
- If $t_i = |Z_i : \mathbb{Q}|$, then the t_i conjugates of χ_i are exactly those characters not annihilating $(D_i)_{d_i}$

- Given a group Γ, a ring R, an action $a : \Gamma \to \mathrm{Aut}(R)$ and a 2-cocycle $t : G \times G \to U(R)$
- we define a generalized crossed product $R *_a^t \Gamma$ as the free R-module $\bigoplus_{g \in \Gamma} Ru_g$ with product $ru_g = u_g r^g$ and $u_g u_h = t(g,h)u_{gh}$
- A cyclotomic algebra is a generalized crossed product with $R = F$ a field, F is a cyclotomic extension of $K = C_F(\Gamma)$, $\Gamma = Gal(F/K)$ and t has roots of unity as values

- Given a group Γ, a ring R, an action $a : \Gamma \to \mathrm{Aut}(R)$ and a 2-cocycle $t : G \times G \to U(R)$
- we define a generalized crossed product $R *_a^t \Gamma$ as the free R-module $\bigoplus_{g \in \Gamma} Ru_g$ with product $ru_g = u_g r^g$ and $u_g u_h = t(g,h)u_{gh}$
- A cyclotomic algebra is a generalized crossed product with $R = F$ a field, F is a cyclotomic extension of $K = C_F(\Gamma)$, $\Gamma = Gal(F/K)$ and t has roots of unity as values

- Given a group Γ, a ring R, an action $a : \Gamma \to \mathrm{Aut}(R)$ and a 2-cocycle $t : G \times G \to U(R)$
- we define a generalized crossed product $R *_a^t \Gamma$ as the free R-module $\bigoplus_{g \in \Gamma} Ru_g$ with product $ru_g = u_g r^g$ and $u_g u_h = t(g, h) u_{gh}$
- A cyclotomic algebra is a generalized crossed product with $R = F$ a field, F is a cyclotomic extension of $K = C_F(\Gamma)$, $\Gamma = Gal(F/K)$ and t has roots of unity as values

- **Theorem (Brauer-Witt 1954)**

  every simple component of $\mathbb{Q}G$ is (Brauer) equivalent to a cyclotomic algebra

  - Olivieri, Olteanu, del Rio, Simon 2003-2007 have implemented an algorithm that finds the cyclotomic algebras associated to $\mathbb{Q}G$
  - Problem Determine when a cyclotomic algebra A is a division algebra or, more generally, find D, d and build an explicit isomorphism with $(D)_d$

- **Theorem (Brauer-Witt 1954)**

  every simple component of $\mathbb{Q}G$ is (Brauer) equivalent to a cyclotomic algebra

  - Olivieri, Olteanu, del Rio, Simon 2003-2007 have implemented an algorithm that finds the cyclotomic algebras associated to $\mathbb{Q}G$
  - Problem Determine when a cyclotomic algebra A is a division algebra or, more generally, find D, d and build an explicit isomorphism with $(D)_d$

- **Theorem (Brauer-Witt 1954)**

  every simple component of $\mathbb{Q}G$ is (Brauer) equivalent to a cyclotomic algebra

  - Olivieri, Olteanu, del Rio, Simon 2003-2007 have implemented an algorithm that finds the cyclotomic algebras associated to $\mathbb{Q}G$
  - Problem Determine when a cyclotomic algebra A is a division algebra or, more generally, find D, d and build an explicit isomorphism with $(D)_d$

- **Theorem (Brauer-Witt 1954)**

  every simple component of $\mathbb{Q}G$ is (Brauer) equivalent to a cyclotomic algebra

  - Olivieri, Olteanu, del Rio, Simon 2003-2007 have implemented an algorithm that finds the cyclotomic algebras associated to $\mathbb{Q}G$
  - Problem Determine when a cyclotomic algebra A is a division algebra or, more generally, find D, d and build an explicit isomorphism with $(D)_d$