On the Number of Representations of a Finite Group over a Finite Field

Pornrat Ruengrot

Mahidol University International College

23 November 2016

Algebraic Structures

Groups, Rings, Division Rings, Fields, Modules, Vector Spaces, Algebras
Very informally (not enough space to write down all the axioms...),

- **Group**: $(G, \cdot)$ Set with binary operation

$$(C_n, \cdot), (\mathbb{R}, \cdot), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}, +), (GL_n(\mathbb{R}), \cdot), (M_n(\mathbb{R}), +)$$

- **Ring**: $(R, +, \cdot)$ where $(R, +)$ abelian group, also has multiplication $(R, \cdot)$ (Needs not be commutative or has multiplicative inverses)

$$(\mathbb{Z}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{Q}[X], +, \cdot), (M_n(\mathbb{R}), +, \cdot)$$

- Ring R with multiplicative inverses $\longrightarrow$ **division ring**

$$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{H}, +, \cdot)$$

$$\mathbb{H} = \{a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} : a, b, c, d \in \mathbb{R}\}$$

Algebraic Structures

- Division ring with multiplication commutative $\longrightarrow$ **field**

$$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{F}_q, +, \cdot)$$

- **Module** M over ring R: $(M, +)$ abelian group, has R as "scalars" or "coefficients"

$$M = \{\sum rm, r \in R, m \in M\}$$

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{R} \cdot 1 + \mathbb{R} \cdot i$$

$$M = \mathbb{Z}m_1 + \mathbb{Z}m_2 + \mathbb{Z}m_3$$

- When R is field F, module over field F is **vector space** over F.

$$\mathbb{R}^n = \mathbb{R}e_1 + \mathbb{R}e_2 + \cdots + \mathbb{R}e_n$$

Algebraic Structures

Algebra A over field F:

- A is vector space over F

$$A = Fa_1 + Fa_2 + \cdots + Fa_n$$

- Can also multiply any two vectors in A. So A is ring.

$$(2a_1 + a_2) \cdot (a_1 - a_2) \quad \text{makes sense}$$

Important example: **group algebra**

$$FG = \{\sum_{g \in G} \lambda_g g : \lambda_g \in F\}$$

Hom-set

$$\mathrm{Hom}_{FG}(V, W)$$

$$T : V \longrightarrow W, T(g \cdot v) = g \cdot T(v) \quad \forall g \in G, \forall v \in V$$

Abelian group with addition (pointwise).
Two FG-modules V_ρ, W_τ are isomorphic if there is an invertible (isomorphism) $T \in \mathrm{Hom}_{FG}(V, W)$. That is,

$$T \circ \rho(g) \circ T^{-1} = \tau(g), \quad \forall g \in G.$$

When $V = W$,

$$\mathrm{Hom}_{FG}(V, V) =: \mathrm{End}_{FG}(V)$$

Multiplication defined by composition:

$$T \cdot S := T \circ S$$

makes $\mathrm{End}_{FG}(V)$ into a ring (**endomorphism ring**).

Schur's lemma

Let V, W be simple FG-modules. Let $T : V \longrightarrow W$ be FG-homomorphism. Then either $T = 0$ or T is isomorphism. In other words,

- If $V \not\simeq W$, then $\mathrm{Hom}_{FG}(V, W) = 0$.
- $\mathrm{End}_{FG}(V)$ is a division ring.

Also, if F is algebraically closed, then $\mathrm{End}_{FG}(V) \simeq F$.

Figure: Issai Schur (1875-1941)

Lemma

Let V be an A-module. Then

$$\mathrm{Hom}_A(A, V) \simeq V.$$

Lemma

(a) $\mathrm{Hom}_A(V, W_1 \oplus W_2) \simeq \mathrm{Hom}_A(V, W_1) \oplus \mathrm{Hom}_A(V, W_2)$

(b) $\mathrm{Hom}_A(V_1 \oplus V_2, W) \simeq \mathrm{Hom}_A(V_1, W) \oplus \mathrm{Hom}_A(V_2, W)$

Lemma

Let $V^{\oplus n} = V \oplus \cdots \oplus V$ (n copies), then

$$\mathrm{End}_A(V^{\oplus n}) \simeq M_n(\mathrm{End}_A(V))$$

as rings.

Number of representations

- G a finite group
- $F = \mathbb{F}_q$ a finite field, $q = p^n$, whose characteristic p does not divide $|G|$
- $GL_n(\mathbb{F}_q) = GL_n(q)$ group of invertible $n \times n$ matrices over $\mathbb{F}_q$

Question

$$|\mathrm{Hom}(G, GL_n(q))| = ?$$

Note that $|\mathrm{Hom}(G, GL_n(q))|$ is finite as $|G|$ and $|GL_n(q)|$ are.

Maschke's Theorem

Let G be a finite group and F a field whose characteristic does not divide $|G|$. Then every left FG-module V is semisimple (completely reducible). That is,

$$V = M_1 \oplus M_2 \oplus \cdots \oplus M_k$$

where M_i's are simple FG-submodules.

Figure: Heinrich Maschke (1853-1908)

Krull-Schmidt theorem

Let G be a finite group, F a field. If V is a finite dimensional FG-module, then

$$V = V_1 \oplus \cdots \oplus V_k$$

where each V_i is an indecomposable FG-module. Furthermore, if

$$V = U_1 \oplus \cdots \oplus U_m$$

is another decomposition with each U_i indecomposable FG-module, then $k = m$ and the summands U_i, V_j are isomorphic in pairs when taken in a suitable order.

Orbit-Stabilizer theorem

Suppose a finite group G acts on a finite set X. Let $x \in X$. Then

$$|Orb(x)| = \frac{|G|}{|Stab(x)|}$$

Wedderburn's little theorem

Every finite division ring is a (finite) field.

Figure: Joseph Wedderburn (1882-1948)

Theorem (Chigira, Takegahara, (2000))

Let G be a finite group. Let $F = \mathbb{F}_q$ and suppose the characteristic of F does not divide $|G|$. Let $\{V_1, \ldots, V_r\}$ be a set of representatives of the isomorphism classes of simple FG-modules. For each i with $1 \leq i \leq r$, let $d_i = \dim_F(V_i)$ and $e_i = \dim_F(\mathrm{End}_{FG}(V_i))$. Then

$$|\mathrm{Hom}(G, GL_n(q))| = \sum_{(n_1,\ldots,n_r)} \frac{|GL_n(q)|}{\prod_{i=1}^{r} |GL_{n_i}(q^{e_i})|}$$

where the sum runs over all sequences $(n_1, \ldots, n_r)$ of nonnegative integers satisfying $d_1 n_1 + \cdots + d_r n_r = n$, and $GL_0(q) = \{1\}$.

Note:

$$|GL_n(q)| = \prod_{i=1}^{n-1} (q^n - q^i).$$

Theorem (Liebeck, Shalev (2004))

Let G be a finite group of order N, q a power of a prime p not dividing N and n a positive integer. Then there is an absolute constant c, and a number $d = d(N)$ depending only on N such that

$$cq^{-N^2}\,|GL_n(q)|^{1-N^{-1}} < |\mathrm{Hom}(G, GL_n(q))| < d\,|GL_n(q)|^{1-N^{-1}}$$

Prof. M. W. Liebeck

- Room No : **665**
- Telephone No. : **+44 207 594 8490**
- E-Mail Address : **m.liebeck at imperial.ac.uk**

When G is cyclic

Let $G = C_k = \langle g \rangle$, $F = \mathbb{F}_q$. In this case, a representation of $\rho : G \longrightarrow GL_n(q)$ is completely determine by

$$\rho(g) \quad \text{where } \rho(g)^k = I.$$

Thus

$$\begin{aligned} |Hom(G, GL_n(q))| &= \#\{X \in GL_n(q) : X^k = I\} \\ &= \#\{X \in M_n(\mathbb{F}_q) : X^k = I\} \end{aligned}$$

Example

Let $k = 2$, $q = 3$. Representations of C_2 on $GL_n(3)$. Let

$$a_n = \#\{X \in M_n(\mathbb{F}_3) : X^2 = I\}$$

- $a_1 = 2$
- $a_2 = 14$
- $a_n =$ A053846 (https://oeis.org/A053846)

  $2, 14, 236, 12692, 1783784, 811523288, 995733306992, \ldots$

Theorem (Artin-Wedderburn)

Let A be a finite dimensional algebra over a field F with the property that every finite dimensional module is semisimple. Then A is a direct sum of matrix algebras over division rings. Specifically, if

$$A \simeq V_1^{\oplus n_1} \oplus \cdots \oplus V_r^{\oplus n_r}$$

where V_i's are non-isomorphic simple A-modules, then

$$A \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r)$$

where $D_i = \mathrm{End}_A(V_i)^{op}$.

Theorem

Let G be a cyclic group C_k. Let $F = \mathbb{F}_q$ where $(q, k) = 1$. Suppose

$$X^k - 1 = \prod_i m_i(X)$$

where each $m_i(X) \in F[X]$ is irreducible. Let $d_i = \deg(m_i[X])$. Then

$$|\mathrm{Hom}(C_k, GL_n(q))| = \sum_{(n_1,\ldots,n_r)} \frac{|GL_n(q)|}{\prod_{i=1}^{r} |GL_{n_i}(q^{d_i})|}$$

where the sum runs over all sequences $(n_1, \ldots, n_r)$ of nonnegative integers satisfying $d_1 n_1 + \cdots + d_r n_r = n$, and $GL_0(q) = \{1\}$.

Previous example

Let $k = 2$, $q = 3$. Representations of C_2 on $GL_n(3)$. Let

$$a_n = \#\{X \in M_n(\mathbb{F}_3) : X^2 = I\}$$

In $\mathbb{F}_3$, the polynomial $X^2 = 1$ factors as

$$X^2 - 1 = (X - 1)(X + 1) = (X + 2)(X + 1)$$

Thus, degrees of irreducible FG-modules are: $d_1 = 1, d_2 = 1$. Thus

$$|\mathrm{Hom}(C_2, GL_n(3))| = \sum_{n_1+n_2=n} \frac{|GL_n(3)|}{|GL_{n_1}(3)|\,|GL_{n_2}(3)|}$$

$$2, 14, 236, 12692, 1783784, 811523288, 995733306992, \ldots$$

More examples

- $\#\{X \in M_n(\mathbb{F}_3) : X^4 = I\}$ This is sequence A053848

$$2, 20, 1640, 901424, 1333386848, 9762556479680, \ldots$$

- $\#\{X \in M_n(\mathbb{F}_4) : X^5 = I\}$ This is sequence A053860

$$1, 25, 8065, 15450625, 1157871796225, 879662773819146 25, \ldots$$

- $\#\{X \in M_n(\mathbb{F}_3) : X^{10} = I\}$ This is sequence A053855

$$2, 14, 236, 619220, 11890945640, 613445895807320, \ldots$$

Theorem (Galois group is cyclic)

Let q be a power of prime. For every integer $n \geq 1$, $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a Galois extension and $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic with generator the q-th power map $\sigma_q : x \mapsto x^q$.

Thank you!