Представления конечных групп

Литература:
1. Ж.-П. Серр. Линейные представления конечных групп.
2. Э. Винберг. Линейные представления групп.
3. С. Ленг. Алгебра (гл. 18)
4. Ю. Дрозд, В. Кириченко. Конечномерные алгебры.
5. Ч. Кэртис, И. Райнер. Теория представлений конечных групп и ассоциативных алгебр.

Вводные определения

Зафиксируем поле F (т.наз. *основное поле*). Пусть G — (конечная) группа, V — линейное пространство над F. Напомним, что $GL(V)$ — это группа всех невырожденных линейных операторов в пространстве V.

Определение 1. *Представление группы G в пространстве V* — это гомоморфизм $r : G \to GL(V)$.

Терминология: V — *пространство представления*, $r(g)$ (где $g \in G$) — *операторы представления*, $\dim V$ — *размерность* (иногда говорят *степень*) *представления*. Если не оговорено противное, то наши представления будут конечномерными, а основным полем будет поле $\mathbb{C}$.

Выбирая базис в n-мерном пространстве V, мы получаем изоморфизмы $V \cong F^n$ и $GL(V) \cong GL(n, F)$; здесь $GL(n, F)$ — это группа всех невырожденных $n \times n$-матриц с элементами из поля F. Таким образом, можно говорить о представлениях и как о гомоморфизмах $r : G \to GL(n, F)$ (иногда эти последние называют *матричными* представлениями, отличая их от *операторных*).

Опишем сразу понятие, эквивалентное понятию представления: G-модули.

Определение 2. *G-модуль* — это векторное F-пространство V с заданным в нем F-линейным действием группы G.

Расшифровка: *действие* G в V — это отображение $G \times V \to V$, $(g, v) \mapsto gv$ такое, что $g_1(g_2v) = (g_1g_2)v$, $1v = v$. Действие F-линейно, если $g(\alpha_1v_1 + \alpha_2v_2) = \alpha_1gv_1 + \alpha_2gv_2$, $\alpha_1, \alpha_2 \in F$. В определении G-модуля подразумевается "зависимость" и от поля F.

Очевидно, задать в пространстве V структуру G-модуля — это все равно что задать в V представление G. В самом деле, перевод с одного языка на другой осуществляется формулой $r(g)v = gv$. (Упр. Проверьте детали!) В дальнейшем язык (представлений или G-модулей) будет выбираться для конкретной задачи из соображений удобства.

Определение 3. *Морфизм* G-модулей V и W — это линейное отображение $\varphi : V \to W$ такое, что $\varphi(gv) = g\varphi(v)$.

На языке представлений аналог морфизмов G-модулей — это сплетающие операторы. Именно, пусть $r : G \to GL(V)$ и $s : G \to GL(W)$ — представления, $\varphi : V \to W$ — линейное отображение.

Определение 4. φ — *сплетающий оператор,* если для всех $g \in G$ коммутативна диаграмма

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ \downarrow{\scriptstyle r(g)} & & \downarrow{\scriptstyle s(g)} \\ V & \xrightarrow{\varphi} & W \end{array}$$

(т.е. $\varphi r(g) = s(g)\varphi$).

Упр. Проверьте, что морфизм G-модулей и сплетающий оператор — это действительно одно и то же (но "на разных языках").

Таким образом, как представления группы G, так и G-модули образуют категории. Эти категории эквивалентны. В частности, можно говорить об изоморфизмах в этих категориях; на языке представлений изоморфные представления часто называют *эквивалентными.* Например, матричные представления, построенные по одному и тому же операторному, но с использованием разных базисов, эквивалентны (но, вообще говоря, не равны). (Упр. Проверьте это!)

Примеры. 1. Тривиальное представление: $r(g) = 1$ для всех $g \in G$ (здесь $1 \in GL(V)$ — единичный оператор).

2. Рассмотрим группу $\mathbb{Z}/n\mathbb{Z}$ (это циклическая группа порядка n). Отображение

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*(= GL(1,\mathbb{C})), k \mapsto e^{2\pi ik/n}$$

задает ее одномерное представление.

3. "Тавтологические" представления: если G является подгруппой в $GL(V)$, то тождественное вложение $G \hookrightarrow GL(V)$ задает представление.

Кстати, говорят, что представление $r : G \to GL(V)$ — *точное*, если r инъективно.

Упр. Докажите, что любая конечная группа обладает точным представлением.

4. Рассмотрим группу S_3. Это группа симметрий правильного треугольника, поэтому возникает ее точное представление $S_3 \to O(\mathbb{R}^2) \subset GL(\mathbb{R}^2)$ (здесь $O(\mathbb{R}^2)$ — группа всех ортогональных операторов в евклидовой плоскости R^2). (Упр. Напишите матрицы операторов представления, выбрав подходящий базис.) Конечно, этот пример обобщается, например, на группу D_n симметрий правильного n-угольника ($D_3 \cong S_3$).

5. $r : \mathbb{Z} \to GL(2,\mathbb{Q})$, $r : k \mapsto \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ — представление.

6. $r : \mathbb{Z}/p\mathbb{Z} \to GL(2,\mathbb{F}_p)$, $r : k \mapsto \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ — представление над полем $\mathbb{F}_p$ (здесь p — простое число, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ — поле из p элементов).

Теперь — несколько "общих" способов конструирования представлений.

7. Пусть G_1, G_2 — группы, $f : G_2 \to G_1$ — гомоморфизм групп, $r : G_1 \to GL(V)$ — представление. Тогда $r \circ f : G_2 \to G_1 \to GL(V)$ — представление. В частности, это применимо в ситуации, когда G_2 — подгруппа в G_1 (а f — тождественное вложение) — это просто *ограничение представления на подгруппу.*

8. Пусть (конечная) группа G действует на (конечном) множестве X. Рассмотрим линейное пространство $\mathrm{Fun}(X)$ всех (комплекснозначных) функций на X. Формула $(gf)(x) = f(g^{-1}x)$ превращает $\mathrm{Fun}(X)$ в G-модуль. (Упр. Проверьте это!)

С другой стороны, рассмотрим линейное пространство $\mathbb{C}X$, формально натянутое на X. Продолжая действие G на X по линейности, мы получаем на $\mathbb{C}X$ структуру G-модуля.

Легко проверить (Упр. проверьте!), что очевидный изоморфизм линейных пространств

$$\varphi : \mathrm{Fun}(X) \to \mathbb{C}X,\ \varphi : f \mapsto \sum_{x \in X} f(x) \cdot x$$

оказывается изоморфизмом G-модулей. (Отметим, что G-модули $\mathrm{Fun}(X)$ и $\mathbb{C}X$ определены и для бесконечных множеств X, но они, как правило, не изоморфны.)

Упр. Рассмотрим "тавтологическое" действие группы S_n на множестве $X = \{1, 2, \ldots, n\}$. Напишите матрицы (в подходящем базисе) операторов соответствующего представления S_n в пространстве $\mathrm{Fun}(X) \cong \mathbb{C}X$.

Упр. Проверьте, что представление из предыдущего упражнения точно. Вообще, при каком условии на действие G на X соответствующее представление G в пространстве $\mathrm{Fun}(X) \cong \mathbb{C}X$ будет точным?

Пусть теперь X и Y — конечные множества с заданным в них действием конечной группы G, $\psi : X \to Y$ — *морфизм действий* (= *G-эквивариантное отображение*), т.е. $\psi(gx) = g\psi(x)$. Легко проверить (Упр. проверьте!), что отображение $\psi^* : \mathrm{Fun}(Y) \to \mathrm{Fun}(X)$, $(\psi^* f)(x) = f(\psi(x))$, является морфизмом G-модулей. С другой стороны, продолжая ψ по линейности, мы получаем морфизм G-модулей $\psi_* : \mathbb{C}X \to \mathbb{C}Y$ (проверьте, что на языке функций

$$\psi_* : \mathrm{Fun}(X) \to \mathrm{Fun}(Y),\ (\psi^* f)(y) = \sum_{x \in \psi^{-1}(y)} f(x);$$

конечность множеств X и Y здесь отбросить нельзя!). Если ψ — изоморфизм, то, очевидно, $\psi^* = \psi_*^{-1}$, т.е. G-модули $\mathrm{Fun}(X)$ и $\mathrm{Fun}(Y)$ изоморфны. Упр. Вычислите $\psi^*\psi_*$ и $\psi_*\psi^*$ в общем случае.

9. Рассмотрим важный частный случай конструкций из предыдущего примера. Именно, рассмотрим действие группы G на себе левыми сдвигами (т.е. $(g, x) \mapsto gx$) и правыми сдвигами (т.е. $(g, x) \mapsto xg^{-1}$). Отображение $x \mapsto x^{-1}$ задает изоморфизм между этими действиями (Упр. проверьте!). Таким образом, соответствующие представления G в пространстве $\mathrm{Fun}(G)$ (или в пространстве $\mathbb{C}G$) изоморфны, т.е. по существу это одно и то же представление. Это представление называется (левым или правым) *регулярным представлением* группы G (на другом языке говорят, что G-модуль $\mathrm{Fun}(G) \cong \mathbb{C}G$ — это *регулярный G-модуль*).

Пусть V и V' — два G-модуля. Обозначим через $\mathrm{Hom}_G(V,V')$ пространство всех морфизмов G-модулей $\varphi : V \to V'$. Это действительно линейное подпространство в линейном пространстве $\mathrm{Hom}(V,V')$ всех линейных отображений из V в V'. Отметим, что $\mathrm{End}_G V = \mathrm{Hom}_G(V,V)$ — это алгебра (что это?), причем $\mathrm{Hom}_G(V,V')$ является левым $\mathrm{End}_G V'$-модулем и правым $\mathrm{End}_G V$-модулем (почему?).

Число $c(V,V') = \dim \mathrm{Hom}_G(V,V')$ называется *числом сплетения* G-модулей (представлений) V и V'. Будем писать $c(V)$ вместо $c(V,V)$.

Упр. Пусть конечная группа G действует на конечных множествах X и Y. Опишите пространство $\mathrm{Hom}_G(\mathrm{Fun}(X),\mathrm{Fun}(Y))$. Покажите, что $c(\mathrm{Fun}(X),\mathrm{Fun}(Y))$ равно числу орбит диагонального действия G на множестве $X \times Y$ (т.е. G действует на $X \times Y$ так: $g(x,y) = (gx, gy)$). В частности, $c(\mathrm{Fun}(G)) = |G|$.

Пусть V — G-модуль.

Определение 5. *G-подмодуль в V* — это линейное подпространство $L \subset V$ такое, что $gL \subset L$ для всех $g \in G$.

Конечно, G-подмодуль сам по себе является G-модулем. На языке представлений это приводит к понятию подпредставления, т.е. подпространства в пространстве представления, инвариантного относительно всех операторов представления.

Очевидно, что сумма и пересечение G-подмодулей — G-подмодуль.

Пусть V — G-модуль, $L \subset V$ — G-подмодуль. Формула $g(v+L) = gv + L$ корректно определяет на факторпространстве V/L структуру G-модуля; он называется фактормодулем (V по L).

Упр. Пусть конечная группа G действует на конечном множестве X. Проверьте, что одномерное подпространство констант — G-подмодуль в $\mathrm{Fun}(X)$. Опишите соответствующий фактормодуль.

Упр. Если $\varphi \in \mathrm{Hom}_G(V,V')$, то $\mathrm{Ker}\varphi \subset V$ и $\mathrm{Im}\varphi \subset V'$ — G-подмодули, причем $V/\mathrm{Ker}\varphi \cong \mathrm{Im}\varphi$.

Упр. Пусть L и M — G-подмодули некоторого G-модуля. Постройте естественный изоморфизм $L/L \cap M \cong (L+M)/M$.

Если V_1 и V_2 — G-модули, то на пространстве $V_1 \oplus V_2$ имеется естественная структура G-модуля; она задается формулой $g(v_1+v_2) = gv_1 + gv_2$. (Мы не будем явно различать “внутреннюю” и “внешнюю” прямые суммы.)

Упр. Пусть конечная группа G действует на конечном множестве X. Проверьте, что одномерный подмодуль L функций-констант в $\mathrm{Fun}(X)$ обладает дополнительным подмодулем M (т.е. $\mathrm{Fun}(X) = L \oplus M$). Что это за подмодуль?

Неприводимость

В этом разделе мы не накладываем никаких условий на основное поле (если не оговорено противное).

Пусть V — G-модуль.

Определение 6. V *приводим,* если в V существует нетривиальный G-подмодуль (нетривиальный = не равный 0 и V). V *неприводим,* если V не является приводимым и $V \neq 0$. (Т.е. нулевой G-модуль не является ни приводимым, ни неприводимым.)

На языке представлений приводимость представления $r : G \to GL(V)$ означает наличие нетривиального подпространства в V, инвариантного относительно всех операторов представления $r(g)$. А что это означает на "матричном" языке?

На языке G-модулей вместо "неприводимый G-модуль" часто (и даже чаще!) говорят "*простой* G-модуль".

Определение 7. G-модуль V *разложим,* если $V = L_1 \oplus L_2$, где L_1 и L_2 — нетривиальные G-подмодули. V *неразложим,* если V не является разложимым и $V \neq 0$. (Снова нулевой G-модуль не считается ни разложимым, ни неразложимым.)

Упр. Что такое "разложимость" на языке представлений?

Очевидно, разложимость $\Rightarrow$ приводимость, неприводимость $\Rightarrow$ неразложимость.

Примеры. 1. Одномерные представления, очевидно, неприводимы.

2. Естественное двумерное представление группы S_3 (интерпретируемой как группа симметрий правильного треугольника) неприводимо (над $\mathbb{C}$, а тем более и над $\mathbb{R}$ или $\mathbb{Q}$...).

3. Рассмотрим двумерное представление группы $\mathbb{Z}/n\mathbb{Z}$, заданное формулой

$$k \mapsto \begin{pmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}.$$

(Это представление соответствует интерпретации $\mathbb{Z}/n\mathbb{Z}$ как группы вращений правильного n-угольника.) Оно неприводимо над $\mathbb{R}$ (если только $n \geq 3$). Однако оно (точнее, его комплексификация) приводимо (и даже разложимо) над $\mathbb{C}$ (почему?).

4. Представление $r : \mathbb{Z} \to GL(2, \mathbb{Q})$, $r : k \mapsto \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ приводимо, но неразложимо даже над $\mathbb{C}$ (почему?). То же относится и к представлению $r : \mathbb{Z}/p\mathbb{Z} \to GL(2, \mathbb{F}_p)$, $r : k \mapsto \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ над полем $\mathbb{F}_p$.

Будет показано, что для конечномерных представлений конечных групп над полем комплексных чисел неприводимость равносильна неразложимости (в этом утверждении поле $\mathbb{C}$ можно заменить на любое поле F при условии, что $\mathrm{char}F$ не делит $|G|$).

Пусть V — неприводимый G-модуль. Что можно сказать об алгебре $\mathrm{End}_G V$?

Предложение 1. (Лемма Шура) *$End_G V$ — тело. (Т.е. все ненулевые эндоморфизмы V — автоморфизмы.)*

Доказательство. Пусть $\varphi \in \mathrm{End}_G V$, $\varphi \neq 0$. Так как $\mathrm{Ker}\varphi$ — G-подмодуль в V, то (неприводимость!) $\mathrm{Ker}\varphi = 0$, т.е. φ инъективен. $\mathrm{Im}\varphi$ также является G-подмодулем, поэтому $\mathrm{Im}\varphi = V$, т.е. φ сюръективен. □

Конечно, точно так же доказывается, что любой ненулевой морфизм из неприводимого G-модуля (соотв. в неприводимый G-модуль) инъективен (соотв. сюръективен). В частности, ненулевой морфизм между (a priori различными) неприводимыми G-модулями является изоморфизмом.

Пусть снова V — неприводимый G-модуль. Отметим, что $\mathrm{End}_G V$ — не только тело, но и алгебра над основным полем F. Попросту говоря, F содержится в центре тела $\mathrm{End}_G V$ (F вкладывается в $\mathrm{End}_G V$ так: $\alpha \mapsto \alpha \cdot 1$). В такой ситуации коротко говорят, что $\mathrm{End}_G V$ — тело над F. В нашем случае, когда V вдобавок конечномерен, то тело $\mathrm{End}_G V$ тоже конечномерно над F.

В лемме Шура (в ее предыдущем виде) не нужны никакие условия на основное поле (а также конечность группы и конечномерность модулей...). Если же основное поле алгебраически замкнуто, то лемму Шура можно усилить.

Предложение 2. (Лемма Шура №2) *Пусть основное поле F алгебраически замкнуто, V — неприводимый G-модуль. Тогда $End_G V = F \cdot 1$.*

Доказательство. Пусть $\varphi \in \mathrm{End}_G V$. В силу алгебраической замкнутости поля F оператор φ имеет собственное значение $\lambda \in F$, т.е. $\varphi - \lambda \cdot 1$ необратим. Но $\varphi - \lambda \cdot 1 \in \mathrm{End}_G V$, откуда (лемма Шура!) $\varphi - \lambda \cdot 1 = 0$, т.е. $\varphi = \lambda \cdot 1$. □

Упр. Докажите, что если поле F алгебраически замкнуто, то единственное (с точностью до изоморфизма) конечномерное тело над F — это само F. (Контрольный вопрос: почему результату упражнения при $F = \mathbb{C}$ не противоречит тело кватернионов $\mathbb{H}$?)

Вот еще несколько случаев, когда строение конечномерных тел над данным полем просто понять (это не значит, что эти теоремы просто и доказать!).

Факт. **1. (Теорема Фробениуса)** Все (с точностью до изоморфизма) конечномерные тела над полем $\mathbb{R}$ — это $\mathbb{R}$, $\mathbb{C}$ и $\mathbb{H}$.
2. (Теорема Веддерберна) Если поле F конечно, то единственное конечномерное центральное тело над F — это само F. (Говорят, что тело *центрально над F*, если F совпадает с центром тела; рассмотрение лишь центральных тел позволяет отделить вопросы теории полей от нашего вопроса о телах (как?). Иначе говоря, теорема Веддерберна гласит, что любое конечное тело коммутативно, т.е. является полем.)
3. (Теорема Тзена) Пусть $F = \Bbbk(x)$, где поле $\Bbbk$ алгебраически замкнуто. Тогда единственное конечномерное центральное тело над F — это само F.

В случае $F = \mathbb{Q}$ задача описания конечномерных центральных тел сводится к важным задачам теории чисел.

Вот первое применение леммы Шура.

Предложение 3. *Всякое неприводимое представление конечной абелевой группы над алгебраически замкнутым полем одномерно.*

Доказательство. Итак, пусть группа G абелева, $r : G \to GL(V)$ — ее неприводимое представление. Для всех $g, h \in G$ имеем $r(g)r(h) = r(h)r(g)$, т.е. все операторы $r(g)$ являются сплетающими для представления r. Согласно лемме Шура №2, все операторы $r(g)$ скалярны, т.е. их матрицы (в любом базисе!) диагональны. Конечно, представление r может быть (и будет!) неприводимым, лишь если $\dim V = 1$. □

Вполне приводимые представления

Предложение 4. *Пусть V — G-модуль. Следующие условия эквивалентны:*
(1) $V = L_1 \oplus L_2 \oplus \ldots \oplus L_m$, *где L_i — неприводимые G-подмодули в V.*
(2) $V = L_1 + L_2 + \ldots + L_m$, *где L_i — неприводимые G-подмодули в V.*
(3) *Всякий G-подмодуль $L \subset V$ дополняем, т.е. существует G-подмодуль L' такой, что $V = L \oplus L'$.*

Определение 8. G-модули, удовлетворяющие условиям предложения 4, называются *вполне приводимыми* (или *полупростыми*).

Упр. Переведите это понятие на язык представлений.

Доказательство предложения 4. (1) $\Rightarrow$ (2): тривиально.

(2) $\Rightarrow$ (3): Пусть (3) не выполнено, т.е. в V существуют недополняемые G-подмодули. Пусть $M \subset V$ — недополняемый G-подмодуль наибольшей размерности. Ясно, что $M \neq V$, поэтому $L_i \not\subseteq M$ для некоторого i. В силу неприводимости L_i мы получаем, что $L_i \cap M = 0$. Таким образом, $M + L_i$ — прямая сумма, т.е. $\dim(M + L_i) > \dim M$. Покажем, что $M \oplus L_i$ тоже недополняем (что противоречит выбору M). В самом деле, его дополняемость означает наличие G-подмодуля $N \subset V$ такого, что $V = M \oplus L_i \oplus N$. Но тогда и M дополняем — противоречие.

(3) $\Rightarrow$ (1): Пусть V не удовлетворяет (1). Выберем в V G-подмодуль L наибольшей размерности, удовлетворяющий (1) (выбирать есть из чего: нулевой G-подмодуль удовлетворяет (1)!). По предположению, $L \neq V$. Вспомним, что L дополняем, т.е. $V = L \oplus L'$, где L' — ненулевой G-подмодуль. Выберем в L' неприводимый G-подмодуль N (он всегда найдется — годится ненулевой подмодуль наименьшей размерности). Но тогда $L + N = L \oplus N$ — прямая сумма, т.е. $\dim(L + N) > \dim L$. Кроме того, $L \oplus N$, очевидно, удовлетворяет (1), что противоречит выбору L. □

Вот наша первая основная теорема:

Теорема 5. (Теорема Машке) *Все конечномерные комплексные представления конечной группы вполне приводимы.*

Доказательство. Пусть G — конечная группа, V — конечномерный G-модуль, $L \subset V$ — G-подмодуль. Достаточно доказать, что L дополняем. Выберем в V какое-нибудь эрмитово скалярное произведение $(\cdot\,,\,\cdot)$. Теперь "усредним его по G", положив $\langle v_1, v_2\rangle = \sum_{g\in G}(gv_1, gv_2)$. Очевидно (кому не очевидно — проверьте!), что эрмитово скалярное произведение $\langle\cdot\,,\,\cdot\rangle$ является G-инвариантным, т.е. $\langle gv_1, gv_2\rangle = \langle v_1, v_2\rangle$ для всех $g \in G$, $v_1, v_2 \in V$. Положим $M = L^\perp$ (ортогональное дополнение берется относительно $\langle\cdot\,,\,\cdot\rangle$!). Ясно, что $V = L \oplus M$. Кроме того, M является G-подмодулем: если $v \in M$, $g \in G$, то $\langle gv, w\rangle = \langle v, g^{-1}w\rangle = 0$ для всех $w \in L$, т.е. $gv \in M$. □

Замечание. Теорема Машке остается верной, если заменить поле $\mathbb{C}$ на любое поле F при условии, что $|G|$ не делится на $\mathrm{char}F$. Вот набросок доказательства, пригодного для этого более общего случая. Пусть снова G — конечная группа, V — конечномерный G-модуль (и $r : G \to GL(V)$ — соответствующее представление), $L \subset V$ — G-подмодуль. Рассмотрим произвольный проектор P на L (вдоль некоторого дополнительного к L подпространства). Теперь усредним P по группе G, положив

$$Q = \frac{1}{|G|}\sum_{g\in G} r(g)Pr(g)^{-1}.$$

Упр. Проверьте, что Q также является проектором на L, причем $Q \in \mathrm{End}_G V$. Кроме того, $\mathrm{Ker}Q \subset V$ — G-подмодуль, дополнительный к L.

Теперь самое время объяснить связь теории представлений групп и теории представлений ассоциативных алгебр.

Пусть, как и прежде, G — конечная группа, F — поле. Рассмотрим линейное F-пространство FG: его элементы — это формальные линейные комбинации элементов G с коэффициентами из F. Превратим FG в G-алгебру, продолжив умножение в G по билинейности:

$$\left(\sum_{g\in G}\alpha_g g\right)\cdot\left(\sum_{h\in G}\beta_h h\right) = \sum_{g,h\in G}\alpha_g\beta_h gh = \sum_{g\in G}\left(\sum_{h_1h_2=g}\alpha_{h_1}\beta_{h_2}\right)g.$$

Алгебра FG называется *групповой алгеброй* группы G.

Отметим, что FG — ассоциативная алгебра с единицей, $\dim FG = |G|$. (Если, как и раньше, отождествить пространство FG с пространством $\mathrm{Fun}(G, F)$, состоящим из F-значных функций на G, то соответствующая операция умножения в $\mathrm{Fun}(G, F)$ называется *сверткой функций* и задается формулой $(f_1 * f_2)(g) = \sum_{h_1h_2=g} f_1(h_1)f_2(h_2)$. С другой стороны, $\mathrm{Fun}(G, F)$ является алгеброй относительно поточечного умножения: $(f_1f_2)(g) = f_1(g)f_2(g)$. Вообще говоря, эти алгебры неизоморфны — например потому,

что вторая всегда коммутативна, а первая не обязательно. Когда говорят "алгебра $\mathrm{Fun}(G,F)$", то по умолчанию предполагают, что это алгебра относительно поточечного умножения. Т.е. мы отождествляем FG и $\mathrm{Fun}(G,F)$ как линейные пространства, но не как алгебры.)

Очевидно, что G-модули (над полем F) и FG-модули — это "одно и то же". (Контрольный вопрос: что такое модуль над ассоциативной алгеброй?) В самом деле, если V является G-модулем, то структура FG-модуля в V задается формулой $\left(\sum_{g\in G}\alpha_g g\right)v = \left(\sum_{g\in G}\alpha_g gv\right)$. Обратно, если V является FG-модулем, то структура G-модуля в V получается "ограничением". (Упр. Проверьте детали!) Более того, морфизмы G-модулей и FG-модулей — это одно и то же (почему?). Т.е. категории G-модулей и FG-модулей "совпадают".

Говорят, что конечномерная ассоциативная алгебра с единицей *полупроста*, если любой конечномерный модуль над ней вполне приводим. Итак, теорема Машке означает, что если группа G конечна, а поле F таково, что $|G|$ не делится на $\mathrm{char}F$, то алгебра FG полупроста (в частности, алгебра $\mathbb{C}G$ полупроста).

Что, если $|G|$ делится на $\mathrm{char}F$? В этом случае алгебра FG действительно не полупроста. Оказывается, регулярное представление не будет вполне приводимым. Проверим это. Рассмотрим (левый) регулярный G-модуль (= FG-модуль) FG. (Отметим, что для любой алгебры A умножение в A превращает пространство A в A-модуль — т.наз. *левый регулярный* A-модуль. Его подмодули — это левые идеалы в A.) Рассмотрим $u := \sum_{g\in G} g \in FG$. Если $g \in G$, то, очевидно, $gu = ug = u$. Таким образом, Fu — двусторонний идеал в FG; в частности, это подмодуль регулярного модуля (на языке функций на группе Fu — это подпространство констант). Если Fu дополняем, то $FG = Fu \oplus L$, где L — левый идеал в FG. Пусть $v \in L$. Так как L — левый идеал, то $uv \in L$. С другой стороны, так как Fu — двусторонний (в частности, правый) идеал, то $uv \in Fu$. Таким образом, $uv = 0$. Теперь заметим, что

$$u^2 = \sum_{g\in G}\Big|\{(h_1,h_2)\in G\times G \,|\, h_1h_2 = g\}\Big|\cdot g = |G|\sum_{g\in G} g = |G|\cdot u.$$

Но если $|G|$ делится на $\mathrm{char}F$, то $|G| = 0$ в поле F, т.е. $u^2 = 0$. Итак, $ux = 0$ для всех $x \in FG$, что абсурдно (ибо $u \neq 0$ и $ug = u$ при $g \in G$).

В случае, когда $|G|$ делится на $\mathrm{char}F$, принят термин "модулярная теория представлений" (или просто "модулярные представления"). Эта теория существенно сложнее "классической" (прежде всего из-за отсутствия полной приводимости); мы не будем ею заниматься.

Упр. Докажите, что если в условиях теоремы Машке ($|G|$ не делится на $\mathrm{char}F$) все неприводимые представления группы G одномерны, то G абелева (Указание: рассмотрите любое точное представление группы G — например, регулярное — и разложите его на неприводимые.)

Пусть G-модуль V вполне приводим. Однозначно ли он разлагается на неприводимые? Оказывается, разложение по существу однозначно (но все же не в буквальном

смысле). Точнее, если $V = L_1 \oplus \ldots \oplus L_m = L'_1 \oplus \ldots \oplus L'_n$, где все подмодули L_i и L_j неприводимы, то $m = n$, и после подходящей перенумерации $L'_i \simeq L_i$ для всех i. Однако неприводимые компоненты, вообще говоря, определены внутри V неоднозначно (т.е. заменить $L'_i \simeq L_i$ на $L'_i = L_i$ нельзя!).

Пример. Рассмотрим "тривиальное" представление $r : G \to GL(V)$ произвольной группы G в n-мерном пространстве V (т.е. $r(g) = 1$ для всех $g \in G$). Очевидно, что $V \simeq L \oplus \ldots \oplus L$ (n слагаемых), где L — тривиальный одномерный G-модуль. Чтобы выбрать определенное разложение V на неприводимые, надо просто взять разложение $V = L_1 \oplus \ldots \oplus L_n$ в прямую сумму одномерных подпространств L_i (ибо для тривиальной структуры G-модуля любое подпространство является G-подмодулем). Если $n > 1$, то в выборе такого разложения имеется большой произвол.

Для доказательства "однозначности" разложения на неприводимые нам понадобятся некоторые вспомогательные факты (полезные и сами по себе). Именно, пусть V, V' и V'' — G-модули.

Упр. 1) Проверьте, что отображение $(\varphi, \psi) \mapsto \chi$, где $\chi(v) = (\varphi(v), \psi(v))$ задает изоморфизм $\mathrm{Hom}_G(V, V') \oplus \mathrm{Hom}_G(V, V'') \simeq \mathrm{Hom}_G(V, V' \oplus V'')$.
2) Проверьте, что отображение $\varphi \mapsto (\varphi|_{V'}, \varphi|_{V''})$ задает изоморфизм $\mathrm{Hom}_G(V' \oplus V'', V) \simeq \mathrm{Hom}_G(V', V) \oplus \mathrm{Hom}_G(V'', V)$.

(Конечно, результат этого упражнения — очень общий: например, буквально то же верно для линейных пространств, абелевых групп и вообще, в любой абелевой категории...)

Из упражнения немедленно вытекает, что функция $c(\cdot\,, \cdot)$ (напомним, что $c(V, V') = \dim \mathrm{Hom}_G(V, V')$) биаддитивна, т.е. $c(V' \oplus V'', V) = c(V', V) \oplus c(V'', V)$, $c(V, V' \oplus V'') = c(V, V') \oplus c(V, V'')$.

Теперь предположим, что основное поле алгебраически замкнуто. Пусть $V = L_1 \oplus \ldots \oplus L_m$, где все L_i — неприводимые G-модули. Пусть L — также неприводимый G-модуль. Согласно лемме Шура, $c(L, L_i) = 1$, если $L_i \simeq L$, и $c(L, L_i) = 0$, если $L_i \not\simeq L$. Поэтому

$$c(L, V) = c(L, L_1) + \ldots + c(L, L_n) = \Big|\{i \mid L_i \simeq L\}\Big|.$$

Так как число $c(L, V)$ не зависит от произвола в выборе разложения V на неприводимые, то однозначность такого разложения (в указанном выше смысле) доказана. (Попросту говоря, мы проверили, что $c(L, V)$ — это число вхождения L в разложение V на неприводимые.)

Однозначность разложения на неприводимые имеет место и в случае любого поля (и даже в модулярном случае, если вы стартуете с вполне приводимого G-модуля), но мы не будем давать общее доказательство. На самом деле все это — частные случаи очень общей теоремы Крулля-Шмидта (см., например, у Кэртиса и Райнера).

Упр. Проверьте, что функция $c(\cdot\,, \cdot)$ симметрична, т.е. $c(V, V') = c(V', V)$. (Предполагайте, что группа конечна, модули конечномерны, а основное поле алгебраически замкнуто.)

Оказывается, что в разложении вполне приводимого G-модуля V на неприводимые сумма всех слагаемых, изоморфных данному неприводимому G-модулю, определена однозначно как подмодуль в V (т.е. не зависит от выбора разложения).

Именно, пусть L — неприводимый G-модуль. Положим

$$V_L = \sum_{M \subset V,\, M \simeq L} M.$$

Говорят, что V_L — это *L-изотипическая компонента V*. (Если в V нет подмодулей, изоморфных L, то полагают $V_L = 0$.) Очевидно, V_L зависит только от класса изоморфизма G-модуля L.

Полная приводимость, очевидно, означает, что $V = \sum_L V_L$ (здесь L пробегает множество представителей классов изоморфизма неприводимых L-модулей). На самом деле сумма прямая.

Предложение 6. $V = \bigoplus_L V_L$.

Доказательство. Зафиксируем неприводимый G-модуль L. Пусть $V = L_1 \oplus \ldots \oplus L_s \oplus L_{s+1} \oplus \ldots$ — разложение на неприводимые, пронумерованное так, что $L \simeq L_1 \simeq \ldots \simeq L_s$, $L_k \not\simeq L$ при $k > s$. Достаточно проверить, что $V_L = L_1 \oplus \ldots \oplus L_s$. Включение "$\supset$" следует из определения. Наоборот, пусть $M \subset V$, $M \simeq L$. Почему $M \subset L_1 \oplus \ldots \oplus L_s$? Ясно, что M — это образ L при некотором гомоморфизме G-модулей $\varphi : L \to V$. Но $\mathrm{Hom}_G(L, V) = \mathrm{Hom}_G(L, L_1 \oplus \ldots \oplus L_s) \oplus \mathrm{Hom}_G(L, L_{s+1}) \oplus \ldots = \mathrm{Hom}_G(L, L_1 \oplus \ldots \oplus L_s)$ (ибо по лемме Шура $\mathrm{Hom}_G(L, L_k) = 0$ при $k > s$). Т.е. $M = \mathrm{Im}\varphi \subset L_1 \oplus \ldots \oplus L_s$. $\square$

Случай абелевых групп

В этом разделе все группы будут абелевыми, а основное поле — это $\mathbb{C}$.

Итак, пусть G — конечная абелева группа. Мы видели, что все ее неприводимые представления одномерны (т.е. попросту являются гомоморфизмами $G \to \mathbb{C}^*$). Эти представления называют еще *(линейными) характерами* группы G. Напомним, что если $|G| = n$, то $g^n = 1$ для всех $g \in G$. Поэтому значения любого характера группы G — это корни n-й степени из 1 (и уж тем более эти значения лежат в подгруппе $\mathbb{T} = \{z \in \mathbb{C}^* \,|\, |z| = 1\}$ группы $\mathbb{C}^*$).

Обозначим через $\widehat{G}$ множество всех характеров группы G. На $\widehat{G}$, в свою очередь, имеется естественная структура абелевой группы: если $\chi_1, \chi_2 \in \widehat{G}$, то $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$. (Упр. Проверьте корректность определения и то, что $\widehat{G}$ — абелева группа.) Отметим, что $\chi^{-1}(g) = \overline{\chi(g)}$. Очевидно, что группа $\widehat{G}$ также конечна. Она называется *группой характеров G* (или группой, *двойственной* к G).

Пример. Пусть G — циклическая группа порядка n, т.е. $G = \langle a \,|\, a^n = 1\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Вычислим группу $\widehat{G}$. Очевидно, что любой характер χ группы G однозначно восстанавливается по числу $\chi(a)$, причем отображение $\chi \mapsto \chi(a)$ задает изоморфизм $\widehat{G} \simeq \mu_n$,

где μ_n — группа (комплексных) корней n-й степени из 1. Так как μ_n — тоже циклическая группа порядка n, то $\widehat{G} \simeq G$. Отметим сразу, что этот изоморфизм "неканонический": он зависит от выбора образующей в G (по-другому, от способа отождествления G с μ_n).

Упр. Проверьте, что отображение $(\chi_1, \chi_2) \mapsto \chi$, где $\chi(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$, является изоморфизмом $\widehat{G}_1 \times \widehat{G}_2 \simeq \widehat{G_1 \times G_2}$.

Напомним, что любая конечная абелева группа изоморфна прямому произведению циклических групп. (Однако выбор такого разложения отнюдь не однозначен!) Комбинируя этот факт с предыдущим упражнением и вычислением группы характеров циклической группы, мы получаем

Предложение 7. $\widehat{G} \simeq G$. □

Снова отметим, что этот изоморфизм "неканонический": в его выборе имеется большой произвол. Отметим еще, что понятие "группа характеров" можно обобщить на случай т.наз. локально компактных абелевых групп (там важную роль начинают играть и топологические вопросы), и для них такого изоморфизма, вообще говоря, нет. (Например, можно показать, что $\widehat{\mathbb{Z}} \simeq \mathbb{T}$, $\widehat{\mathbb{T}} \simeq \mathbb{Z}$, $\widehat{\mathbb{R}} \simeq \mathbb{R}$.)

Так как $\widehat{G} \simeq G$, то, конечно, $\widehat{\widehat{G}} \simeq G$. Но оказывается, что $\widehat{\widehat{G}}$ и G связаны каноническим изоморфизмом (не зависящим ни от каких произвольных выборов). Слово "канонический" можно охарактеризовать и более точно: этот изоморфизм на самом деле индуцирует изоморфизм функтора "двойной крышки" и тождественного функтора (в категории конечных абелевых групп). Этот факт обобщается и на случай локально компактных абелевых групп (т.наз. *двойственность Понтрягина*).

Именно, пусть $g \in G$. Сопоставим g функцию f_g на группе $\widehat{G}$, определенную формулой $f_g(\chi) = \chi(g)$. Очевидно (Упр. проверьте честно, если вам не очевидно...), что $f_g \in \widehat{\widehat{G}}$, и $g \mapsto f_g$ — гомоморфизм $G \to \widehat{\widehat{G}}$.

Теорема 8. *Гомоморфизм $g \mapsto f_g$ является изоморфизмом групп G и $\widehat{\widehat{G}}$.*

Обычно просто отождествляют G и $\widehat{\widehat{G}}$ с помощью этого изоморфизма.

Доказательство. Достаточно доказать инъективность нашего гомоморфизма (ибо мы знаем, что $|\widehat{\widehat{G}}| = |G|$). Итак, пусть $g \in G$, $g \neq 1$. Надо показать, что $f_g \neq 1$, т.е. найдется $\chi \in \widehat{G}$ такой, что $\chi(g) \neq 1$. В самом деле, выберем в G циклические подгруппы $G_1, \ldots, G_m$ такие, что $G = G_1 \times \ldots \times G_m$. Тогда $g = g_1 \ldots g_m$, где $g_i \in G_i$, причем $g_j \neq 1$ для некоторого j. Выберем $\chi_j \in \widehat{G}_j$ такой, что χ_j задает изоморфизм G_j и μ_n (здесь, конечно, $n = |G_j|$), и определим $\chi \in \widehat{G}$ формулой $\chi(h_1 \ldots h_m) = \chi_j(h_j)$ (здесь $h_i \in G_i$). Тогда $\chi(g) \neq 1$. □

Лемма 9. *(i) Пусть* $\chi \in \widehat{G}$. *Тогда*

$$\sum_{g\in G}\chi(g) = \begin{cases} |G|, & \text{если } \chi = 1 \\ 0, & \text{если } \chi \neq 1. \end{cases}$$

(ii) Пусть $g \in G$. *Тогда*

$$\sum_{\chi\in\widehat{G}}\chi(g) = \begin{cases} |G|, & \text{если } g = 1 \\ 0, & \text{если } g \neq 1. \end{cases}$$

Доказательство. Утверждения (i) и (ii) получаются друг из друга применением теоремы двойственности, поэтому достаточно доказать, например, (i). Пусть $A = \sum_{g\in G}\chi(g)$. Если $\chi = 1$, то доказывать нечего. Далее, заметим, что $\chi(g)A = A$ для всех $g \in G$. Если $\chi \neq 1$, то выберем g так, чтобы $\chi(g) \neq 1$. Тогда ясно, что $A = 0$. □

Рассмотрим пространство $\mathrm{Fun}(G) = \mathrm{Fun}(G, \mathbb{C})$ и наделим его эрмитовым скалярным произведением по формуле

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f_2(g)}.$$

Отметим, что базис из "δ-функций" является ортогональным (правда, не нормированным) относительно этого скалярного произведения.

Предложение 10. (соотношения ортогональности для характеров) *(i)* $\widehat{G}$ — *ортонормированный базис в пространстве* $Fun(G)$; *т.е. если* $\chi_1, \chi_2 \in \widehat{G}$, *то*

$$\frac{1}{|G|}\sum_{g\in G}\chi_1(g)\overline{\chi_2(g)} = \begin{cases} 1, & \text{если } \chi_1 = \chi_2 \\ 0, & \text{если } \chi_1 \neq \chi_2. \end{cases}$$

(ii) Если $g_1, g_2 \in G$, *то*

$$\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(g_1)\overline{\chi(g_2)} = \begin{cases} 1, & \text{если } g_1 = g_2 \\ 0, & \text{если } g_1 \neq g_2. \end{cases}$$

Доказательство. Чтобы доказать, скажем, (i), достаточно применить Лемму 9 к характеру $\chi_1\chi_2^{-1}$. □

Определение 9. *Преобразование Фурье* на G — это линейное отображение $\mathrm{Fun}(G) \to \mathrm{Fun}(\widehat{G})$, $f \mapsto \hat{f}$, заданное формулой $\hat{f}(\chi) = \sum_{g\in G} f(g)\chi(g)$.

Отметим, что наше понятие преобразования Фурье вполне аналогично "классическому": если f — "хорошая" функция на вещественной оси, то

$$\hat{f}(\xi) = \int_{\mathbb{R}} f(x)\chi_\xi(x)dx,$$

где $\chi_\xi(x) = \exp(i\xi x)$; отметим, что $\chi_\xi : \mathbb{R} \to \mathbb{T}$, и $\chi_\xi(x+y) = \chi_\xi(x)\chi_\xi(y)$, т.е. χ_ξ — "характер" группы $\mathbb{R}$. На самом деле все эти определения преобразования Фурье — частные случаи общего понятия преобразования Фурье на локально компактной абелевой группе.

Пример. Пусть δ — это δ-функция единицы группы G. Тогда $\hat{\delta} = 1$.

Предложение 11. $\widehat{f_1 * f_2} = \hat{f}_1 \hat{f}_2$.

Доказательство.

$$\widehat{f_1 * f_2}(\chi) = \sum_{g \in G} \sum_{h_1 h_2 = g} f_1(h_1) f_2(h_2) \chi(g) = \left(\sum_{h_1 \in G} f_1(h_1)\chi(h_1) \right) \cdot \left(\sum_{h_2 \in G} f_2(h_2)\chi(h_2) \right) =$$
$$= \hat{f}_1(\chi)\hat{f}_2(\chi).$$

□

Обратимо ли отображение $f \mapsto \hat{f}$? Оказывается, да. Возьмем $f \in \mathrm{Fun}(G)$ и разложим ее по базису из характеров: $f = \sum_{\chi \in \widehat{G}} c_\chi \chi$. Тогда (ввиду ортонормированности этого базиса)

$$c_\chi = \langle f, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{\chi(g)} = \frac{1}{|G|} \hat{f}(\chi^{-1}).$$

Итак, доказано

Предложение 12. (формула обращения)

$$f = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi^{-1})\chi.$$

□

Итак, $f \mapsto \hat{f}$ — изоморфизм векторных пространств и даже алгебр $(\mathrm{Fun}(G), *)$ и $(\mathrm{Fun}(\widehat{G}), \cdot)$. В частности, $(\mathrm{Fun}(G), *) \simeq (\mathrm{Fun}(G), \cdot)$.

Предложение 13. (формула Планшереля) $\langle \hat{f}_1, \hat{f}_2 \rangle_{\widehat{G}} = |G| \langle f_1, f_2 \rangle_G$.

Доказательство.

$$\langle \hat{f}_1, \hat{f}_2 \rangle_{\widehat{G}} = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}_1(\chi)\overline{\hat{f}_2(\chi)} = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \sum_{g_1 \in G} \sum_{g_2 \in G} f_1(g_1)\chi(g_1)\overline{f_2(g_2)\chi(g_2)} =$$
$$= \sum_{g \in G} f_1(g)\overline{f_2(g)} = |G| \langle f_1, f_2 \rangle_G.$$

□

Итак, преобразование Фурье — это, с точностью до скалярного множителя, унитарное преобразование.

Преобразование Фурье часто возникает при решении различных задач. Например, оно, по сути дела, появляется в одном (а всего их имеется несколько десятков!) доказательств знаменитого квадратичного закона взаимности из теории чисел. Обсудим это.

Итак, пусть p — нечетное простое число. Рассмотрим поле $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Пусть $a \in \mathbb{F}_p^*$. Когда уравнение $x^2 = a$ имеет решение в поле $\mathbb{F}_p$? Положим

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если уравнение } x^2 = a \text{ имеет решение в поле } \mathbb{F}_p, \\ -1, & \text{если уравнение } x^2 = a \text{ не имеет решений в поле } \mathbb{F}_p. \end{cases}$$

Число $\left(\frac{a}{p}\right)$ называется *символом Лежандра* a ("по модулю p"). Как вычислять символ Лежандра?

Упр. 1. $a^{\frac{p-1}{2}} = \pm 1$ для всех $a \in \mathbb{F}_p^*$. 2. $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ для всех $a \in \mathbb{F}_p^*$.

В частности, $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* \to \{1, -1\}$ — гомоморфизм групп.

На "языке целых чисел" мы интересуемся разрешимостью сравнения $x^2 \equiv m \bmod p$, где m — целое число, $p \nmid m$ (если $p \mid m$, то наше сравнение, очевидно, разрешимо...). Положим $\left(\frac{m}{p}\right) = \left(\frac{\bar{m}}{p}\right)$, где $\bar{m}$ — это образ m в $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Тогда, очевидно,

$$\left(\frac{m}{p}\right) = \begin{cases} 1, & \text{если сравнение } x^2 \equiv m \bmod p \text{ имеет решение}, \\ -1, & \text{если сравнение } x^2 \equiv m \bmod p \text{ не имеет решений}. \end{cases}$$

и $\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \bmod p$. Последнее сравнение позволяет вычислять $\left(\frac{m}{p}\right)$, однако это не очень удобно. Удобнее (и экономнее, с точки зрения числа операций) делать это с помощью квадратичного закона взаимности.

Теорема 14. (квадратичный закон взаимности) *Пусть p, q — различные нечетные простые числа. Тогда*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Квадратичный закон взаимности (в сочетании с формулой $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ — вы можете сами подумать, как ее доказать...) позволяет быстро вычислять символ Лежандра. Для этого удобно ввести его обобщение — *символ Якоби*: если $b \in \mathbb{N}$ — нечетное число, $b = p_1 p_2 \dots p_n$, где p_i — простые числа, $m \in \mathbb{Z}$, m взаимно просто с b, то определим

$$\left(\frac{m}{b}\right) := \left(\frac{m}{p_1}\right) \dots \left(\frac{m}{p_n}\right)$$

(в правой части равенства — символы Лежандра). Легко проверить, используя свойства символа Лежандра (Упр. проверьте!), что символ Якоби зависит только от класса вычета "числителя" по модулю "знаменателя", мультипликативен как по "числителю", так и по "знаменателю", а также удовлетворяет тем же свойствам, что и символ Лежандра: $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$, $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$, и если b и c — взаимно простые нечетные натуральные числа, то $\left(\frac{b}{c}\right) = (-1)^{\frac{b-1}{2}\frac{c-1}{2}}\left(\frac{c}{b}\right)$. Однако символ Якоби $\left(\frac{m}{b}\right)$ может равняться 1 и в случае, когда сравнение $x^2 \equiv m \bmod p$ неразрешимо! (Упр. Почему?)

Пример. $\left(\frac{31}{43}\right) = (-1)^{\frac{31-1}{2}\frac{43-1}{2}}\left(\frac{43}{31}\right) = -\left(\frac{43}{31}\right) = -\left(\frac{12}{31}\right) = -\left(\frac{3}{31}\right)\left(\frac{2}{31}\right)^2 = -\left(\frac{3}{31}\right) = -(-1)^{\frac{3-1}{2}\frac{31-1}{2}}\left(\frac{31}{3}\right) = \left(\frac{31}{3}\right) = \left(\frac{1}{3}\right) = 1.$

Контрольный вопрос: зачем вообще вводить символ Якоби, нельзя ли обойтись символом Лежандра? (Ответ: проблема в том, что большие числа трудно разлагать на простые множители, а при использовании символа Якоби достаточно просто выделять множитель 2.)

Как доказать квадратичный закон взаимности? Начнем издалека: рассмотрим т.наз. *квадратичную сумму Гаусса*

$$\mathrm{Gauss} = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \omega^x.$$

Здесь ω — это примитивный корень степени p из 1 (т.е. образующая группы μ_p.) Мы хотим вычислить Gauss^2. (Мы увидим, что это вычисление позволяет доказать квадратичный закон взаимности.)

Рассмотрим сразу и более общую сумму

$$\mathrm{Gauss}_a = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \omega^{ax},$$

где $a \in \mathbb{F}_p$.

Упр. 1. Если $a \neq 0$, то $\mathrm{Gauss}_a = \left(\frac{a}{p}\right)\mathrm{Gauss}$;

2. $\mathrm{Gauss}_0 = 0$;

3. $\overline{\mathrm{Gauss}_a} = \mathrm{Gauss}_{-a}$.

Рассмотрим теперь аддитивную группу поля $\mathbb{F}_p$. Она циклична, и все ее характеры имеют вид $\chi_a(x) = \omega^{ax}$, где $a \in \mathbb{F}_p$. Заметим, что $\mathrm{Gauss}_a = \hat{f}(\chi_a)$, где

$$f(x) = \begin{cases} \left(\frac{x}{p}\right), & \text{если } x \neq 0, \\ 0, & \text{если } x = 0. \end{cases}$$

Применим в нашей ситуации формулу Планшереля. С одной стороны,

$$\|\hat{f}\|^2 = p \cdot \|f\|^2 = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right)^2 = p - 1.$$

С другой стороны,

$$\|\hat{f}\|^2 = \frac{1}{p}\sum_{x\in\mathbb{F}_p}|\mathrm{Gauss}_a|^2 = \frac{1}{p}\sum_{x\in\mathbb{F}_p}\mathrm{Gauss}_a\mathrm{Gauss}_{-a} = \frac{p-1}{p}\left(\frac{-1}{p}\right)\mathrm{Gauss}^2 =$$
$$= \frac{p-1}{p}(-1)^{\frac{p-1}{2}}\mathrm{Gauss}^2.$$

Отсюда $\mathrm{Gauss}^2 = (-1)^{\frac{p-1}{2}}p$.

Теперь перейдем к доказательству квадратичного закона взаимности. Вспомним, что $\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \mod q$. Далее, из нашей формулы для Gauss^2 следует, что $p^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\mathrm{Gauss}^{q-1}$. Осталось вычислить $\mathrm{Gauss}^{q-1} \mod q$.

Упр. Проверьте, что $\mathrm{Gauss}^{q-1} \equiv \left(\frac{q}{p}\right) \mod q$. (Указание. Проверьте вначале, что $\mathrm{Gauss}^q \equiv \left(\frac{q}{p}\right)\mathrm{Gauss} \mod q$. Здесь речь идет о сравнениях в кольце $\overline{\mathbb{Z}}$ целых алгебраических чисел (что это?). Далее, убедитесь, что $\mathrm{Gauss} \not\equiv 0 \mod q$. Чтобы вернуться к сравнениям в $\mathbb{Z}$, воспользуйтесь тем, что $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.)

Итак,

$$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\mathrm{Gauss}^{q-1} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) \mod q,$$

но слева и справа в этом сравнении стоит ± 1, т.е. попросту $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$, что и требовалось доказать.

С идейной точки зрения наши вычисления оказались успешными потому, что нам удалось выразить $\sqrt{p}$ в виде суммы корней из 1. Далее нам понадобилось возводить эту сумму в степень $q-1$ (по модулю q), и не удивительно, что это оказалось несложным: во-первых, возведение в степень q — это гомоморфизм колец в характеристике q; во-вторых, корни из 1 легко возводить в любую степень.

В заключение отметим, что вычисление Gauss^2 означает, что мы знаем Gauss с точностью до знака. Знак тоже можно сосчитать. Можно доказать (это сложнее, чем наше вычисление с точностью до знака), что

$$\mathrm{Gauss} = \begin{cases} \sqrt{p}, & \text{если } p \equiv 1 \mod 4, \\ i\sqrt{p}, & \text{если } p \equiv 3 \mod 4. \end{cases}$$

Об этом можно прочесть, например, в книге Айерлэнда и Роузена “Классическое введение в современную теорию чисел” (гл. 6 и 8). (Там же можно прочитать об обобщениях квадратичной суммы Гаусса и о других применениях всего этого в теории чисел.)

Пусть теперь G — произвольная конечная группа (вообще говоря, не абелева). Как устроены одномерные (комплексные) представления группы G? Отметим сразу, что одномерные представления (как и в абелевом случае) образуют абелеву группу

относительно поточечного умножения. Далее, ясно, что если $\chi : G \to \mathbb{C}^*$ — гомоморфизм, то $\mathrm{Ker}\chi \supset G'$, где G' — коммутант группы G. Иначе говоря, χ пропускается через факторгруппу G/G' (которая, кстати говоря, абелева). Легко проверить, что так получается изоморфизм группы одномерных представлений G на группу $\widehat{G/G'}$.

Пример. Пусть $G = S_n$, $n \geq 3$. Тогда несложно проверить, что $G' = A_n$, и $G/G' \simeq \mathbb{Z}/2\mathbb{Z}$. Таким образом, имеется ровно два одномерных представления группы S_n. Конечно, это 1 и sgn.

Матричные элементы неприводимых представлений

Вернемся к общей теории представлений. Пусть G — конечная группа. Пусть $r : G \to GL(n, \mathbb{C})$ — ее (матричное) представление, $r(g) = (r_{ij}(g))$. Функции $r_{ij} \in \mathrm{Fun}(G)$ называются *матричными элементами* представления r. Отметим, что матричные элементы представления могут поменяться при замене представления на эквивалентное (= изоморфное) ему, т.е. при преобразовании $r(g) \rightsquigarrow T \cdot r(g) \cdot T^{-1}$, где $T \in GL(n, \mathbb{C})$. Однако их линейная оболочка в пространстве $\mathrm{Fun}(G)$ не изменится — почему? (На более инвариантном "операторном" языке это выглядит так: если $r : G \to GL(n, \mathbb{C})$ — представление, то пространство его матричных элементов — это подпространство в $\mathrm{Fun}(G)$, состоящее из функций f вида $f(g) = l(r(g)v)$, где $v \in V$, $l \in V^*$.)

Теперь вспомним, что если $r : G \to GL(n, \mathbb{C})$ — (матричное) представление конечной группы G, то оно эквивалентно *унитарному*, т.е. найдется матрица $T \in GL(n, \mathbb{C})$ такая, что все матрицы $T \cdot r(g) \cdot T^{-1}$ унитарны. (Это следует из доказательства теоремы Машке о полной приводимости.) Поэтому мы можем считать, не ограничивая общности, что наши представления унитарны. Другими словами, мы можем считать, что наши представления — это гомоморфизмы $r : G \to U(n)$, где $U(n)$ — подгруппа в $GL(n, \mathbb{C})$, состоящая из всех унитарных матриц.

Как и прежде, наделим пространство $\mathrm{Fun}(G)$ эрмитовым скалярным произведением по формуле

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

Теорема 15. (соотношения ортогональности для матричных элементов)
(i) Пусть $r : G \to U(m)$ и $s : G \to U(n)$ — неэквивалентные неприводимые унитарные представления. Тогда $\langle r_{ij}, s_{kl} \rangle = 0$ для всех i, j, k, l.
(ii) Пусть $r : G \to U(n)$ — неприводимое унитарное представление. Тогда $\langle r_{ij}, r_{kl} \rangle = 0$ при $(i, j) \neq (k, l)$, и $\langle r_{ij}, r_{ij} \rangle = \frac{1}{n}$.

Доказательство. Сначала — рассуждения, общие для обеих частей теоремы. Пусть $r : G \to U(m)$ и $s : G \to U(n)$ — унитарные представления. Пусть X — произвольная $m \times n$-матрица, $X = (x_{ij})$. Положим

$$A = \frac{1}{|G|} \sum_{g \in G} r(g) X s(g)^{-1}.$$

Ясно, что $r(g)As(g)^{-1} = A$ для всех $g \in G$, т.е. A сплетает представления r и s. Кроме того, легко вычислить, что (i,j)-матричный элемент матрицы $r(g)Xs(g)^{-1}$ равен $\sum_{k,l} r_{ik}(g)\overline{s_{jl}(g)}x_{kl}$. Поэтому $A = (a_{ij})$, где $a_{ij} = \sum_{k,l}\langle r_{ik}, s_{jl}\rangle x_{kl}$.

(i) В этой ситуации $A = 0$, согласно лемме Шура. Так как матрица X произвольна, то наше утверждение доказано.

(ii) (полагаем $s = r$) Теперь по лемме Шура $A = \lambda E$, где $\lambda \in \mathbb{C}$. Тогда $\operatorname{Tr} A = \lambda n$. С другой стороны, $\operatorname{Tr} A = \operatorname{Tr} X = \sum_k x_{kk} = \sum_{kl}\delta_{kl}x_{kl}$. Отсюда $\lambda = \frac{1}{n}\sum_{kl}\delta_{kl}x_{kl}$. Таким образом, $a_{ij} = \lambda\delta_{ij} = \frac{1}{n}\sum_{kl}\delta_{ij}\delta_{kl}x_{kl}$. Сравнивая это с формулой $a_{ij} = \sum_{k,l}\langle r_{ik}, r_{jl}\rangle x_{kl}$, получаем, что $\langle r_{ik}, r_{jl}\rangle = \frac{1}{n}\delta_{ij}\delta_{kl}$, что и требовалось доказать. □

Замечание. Мы доказали, что пространства матричных элементов неприводимых неэквивалентных представлений ортогональны друг другу (и без предположения об унитарности представлений). Кроме того, мы доказали, что размерность пространства матричных элементов неприводимого d-мерного представления равна d^2 (почему?).

Следствие 16. *Множество классов эквивалентности комплексных неприводимых конечномерных предвтавлений конечной группы G конечно.*

Доказательство. Если бы это было не так, то в (конечномерном!) пространстве $\operatorname{Fun}(G)$ существовала бы бесконечная ортогональная (и, стало быть, линейно независимая) система векторов (именно, матричные элементы всех неприводимых представлений). □

Замечание. Пусть G — группа порядка n. Пусть $r_1, \ldots, r_m$ — система представителей классов эквивалентности неприводимых представлений G. Пусть d_i — размерность представления r_i. Тогда размерность пространства матричных элементов представления r_i равна d_i^2. Так как $\dim \operatorname{Fun}(G) = n$, то из взаимной ортогональности пространств матричных элементов представлений r_i следует, что $n \geq d_1 + \ldots + d_m$. Позднее мы увидим, что на самом деле $n = d_1 + \ldots + d_m$.

Характеры

Пусть G — конечная группа, $r : G \to GL(V)$ — ее конечномерное представление.

Определение 10. *Характер* представления r — это функция $\chi_r \in \operatorname{Fun}(G)$, заданная формулой $\chi_r(g) = \operatorname{Tr} r(g)$.

Лемма 17. *Если r — представление группы G в пространстве V, то $\chi_r(1) = \dim V$.*

Доказательство. $\chi_r(1) = \operatorname{Tr}(1_V) = \dim V$. □

Лемма 18. *Если представления $r : G \to GL(V)$ и $s : G \to GL(W)$ изоморфны, то $\chi_r = \chi_s$.*

Доказательство. Изоморфность r и s означает, что существует изоморфизм линейных пространств $\varphi : V \to W$ такой, что $s(g) = \varphi r(g)\varphi^{-1}$. Но тогда $\operatorname{Tr} s(g) = \operatorname{Tr} \varphi r(g)\varphi^{-1} = \operatorname{Tr} r(g)$. □

Пусть теперь $r : G \to GL(V)$ и $s : G \to GL(W)$ — представления. Рассмотрим их прямую сумму, т.е. представление $r \oplus s : G \to GL(V \oplus W)$, заданное формулой $(r \oplus s)(g) : (v, w) \mapsto (r(g)v, s(g)w)$.

Лемма 19. $\chi_{r\oplus s} = \chi_r + \chi_s$.

Доказательство. След прямой суммы линейных операторов равен сумме их следов. □

Будем говорить, что функция $\chi \in \operatorname{Fun}(G)$ — *характер*, если она является характером какого-нибудь представления группы G.

Лемма 20. *Пусть χ — характер. Тогда $\chi(hgh^{-1}) = \chi(g)$.*

Доказательство. Пусть $r : G \to GL(V)$ — представление такое, что $\chi = \chi_r$. Тогда $\chi(hgh^{-1}) = \operatorname{Tr} r(hgh^{-1}) = \operatorname{Tr} r(h)r(g)r(h)^{-1} = \operatorname{Tr} r(g) = \chi(g)$. □

Иначе говоря, характеры являются функциями на G, постоянными на классах сопряженности в G (что это?). Такие функции еще называют функциями классов или центральными функциями. Вот объяснение последнего названия.

Лемма 21. *Функция f принадлежит центру алгебры $(Fun(G), *)$ тогда и только тогда, когда $f(hgh^{-1}) = f(g)$ для всех $g, h \in G$.*

Доказательство. Вспомним, что алгебра $(\operatorname{Fun}(G), *)$ изоморфна групповой алгебре $\mathbb{C}G$, и перейдем на язык $\mathbb{C}G$. Если $\sum_{g\in G} \alpha_g g \in \mathbb{C}G$, $h \in G$, то

$$h^{-1}\left(\sum_{g\in G} \alpha_g g\right) h = \sum_{g\in G} \alpha_g h^{-1}gh = \sum_{g\in G} \alpha_{hgh^{-1}} g.$$

Поэтому $\sum_{g\in G} \alpha_g g$ принадлежит центру алгебры $\mathbb{C}G$ тогда и только тогда, когда $\alpha_{hgh^{-1}} = \alpha_g$ для всех $g, h \in G$. □

Замечание. Итак, базис центра $Z(\mathbb{C}G)$ алгебры $\mathbb{C}G$ образуют, например, элементы $[C] = \sum_{g\in C} g$, где C пробегает множество $\operatorname{Cl}(G)$ классов сопряженности группы G. В частности, $\dim Z(\mathbb{C}G)$ равна числу $\operatorname{cl}(G)$ классов сопряженности группы G.

Таким образом, характеры группы G лкжат в центре алгебры $(\operatorname{Fun}(G), *)$.

Предложение 22. *Пусть r и s — неприводимые конечномерные комплексные представления конечной группы G. Тогда*

$$\langle \chi_r, \chi_s \rangle = \begin{cases} 1, & \text{если } r \text{ и } s \text{ изоморфны,} \\ 0, & \text{если } r \text{ и } s \text{ не изоморфны.} \end{cases}$$

Доказательство. Без ограничения общности мы можем считать наши представления унитарными. Согласно определению, $\chi_r = \sum_i r_{ii}$, $\chi_s = \sum_j s_{jj}$. Если r и s не изоморфны, то $\langle \chi_r, \chi_s \rangle = \sum_{i,j} \langle r_{ii}, s_{jj} \rangle = 0$. Если же r и s изоморфны, то

$$\langle \chi_r, \chi_s \rangle = \langle \chi_r, \chi_r \rangle = \sum_{i,j} \langle r_{ii}, r_{jj} \rangle = \sum_{i=1}^{d} \langle r_{ii}, r_{ii} \rangle = \sum_{i=1}^{d} \frac{1}{d} = 1$$

(здесь d — размерность представления r). □

Замечание. Пусть $r_1, \ldots, r_m$ — система представителей классов эквивалентности неприводимых представлений группы G. Положим $\chi_i = \chi_{r_i}$. Тогда $\langle \chi_i, \chi_j \rangle = \delta_{ij}$, т.е.

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$$

(это — т.наз. *первая система соотношений ортогональности* для характеров неприводимых представлений). Итак, $\chi_1, \ldots, \chi_m$ — ортонормированная система в пространстве $Z(\mathrm{Fun}(G), *)$ (т.е. в центре алгебры $(\mathrm{Fun}(G), *)$). В частности, $m \leq \dim Z(\mathrm{Fun}(G), *) = \mathrm{cl}(G)$. В дальнейшем мы покажем, что $m = \mathrm{cl}(G)$. (Если G абелева, то мы это знаем и так: $m = \mathrm{cl}(G) = |G|$.)

Мы увидим сейчас, что теория характеров позволяет получать разложение данного представления на неприводимые (правда, только “с точностью до изоморфизма”).

Пусть снова $r_1, \ldots, r_m$ — система представителей классов эквивалентности неприводимых представлений группы G. Пусть $\chi_i = \chi_{r_i}$. Если r — представление группы G, то, как мы знаем, $r \simeq k_1 r_1 \oplus \ldots \oplus k_m r_m$ (здесь $k_i r_i$ — прямая сумма k_i экземпляров представления r_i), где числа $k_i \in \mathbb{Z}_+$ определены по r однозначно. Как их найти?

Предложение 23. *Пусть $r \simeq k_1 r_1 \oplus \ldots \oplus k_m r_m$. Тогда $\chi_r = k_1 \chi_1 + \ldots + k_m \chi_m$, причем $k_i = \langle \chi_r, \chi_i \rangle$.*

Доказательство. То, что $\chi_r = k_1 \chi_1 + \ldots + k_m \chi_m$, мы уже проверяли. Далее, из доказанных нами соотношений ортогональности для характеров следует, что $\langle \chi_r, \chi_i \rangle = \sum_j k_j \langle \chi_j, \chi_i \rangle = k_i$. □

Следствие 24. *Представления r и s изоморфны тогда и только тогда, когда $\chi_r = \chi_s$.*

Доказательство. Мы уже доказывали, что если r и s изоморфны, то $\chi_r = \chi_s$. Обратно, если $\chi_r = \chi_s$, то представления r и s “одинаково” разлагаются на неприводимые (см. Предложение 23), и поэтому r и s изоморфны. □

Обычно *неприводимыми характерами* называют характеры неприводимых представлений. Предыдущее следствие показывает, что неприводимый характер не может быть “по совместительству” характером какого-нибудь приводимого представления.

Упр. Пусть χ — характер. Проверьте, что χ неприводим тогда и только тогда, когда $\langle \chi, \chi \rangle = 1$.

Упр. Пусть r и s — представления группы G. Проверьте, что $\langle \chi_r, \chi_s \rangle = c(r, s)$. (Напомним, что $c(r, s)$ — это размерность пространства изоморфизмов между r и s.)

Рассмотрим теперь регулярное представление группы G. Напомним, что это представление "живет" в пространстве $\mathbb{C}G$, и операторы представления — это операторы умножения (слева) на элементы группы G. Мы хотим вычислить его характер. Полезно рассмотреть чуть более общую ситуацию.

Предложение 25. *Пусть конечная группа G действует на конечном множестве X. Пусть χ — характер соответствующего представления группы G в пространстве $\mathbb{C}X$. Тогда $\chi(g) = \Big|\{x \in X \mid gx = x\}\Big|$ (т.е. $\chi(g)$ равно числу неподвижных точек элемента $g \in G$ в множестве X).*

Доказательство. Пронумеруем элементы множества X, т.е. $X = \{x_1, \ldots, x_n\}$. Тогда матрица A оператора представления, соответствующего элементу $g \in G$, в базисе $x_1, \ldots, x_n$ пространства $\mathbb{C}X$, равна (a_{ij}), где

$$a_{ij} = \begin{cases} 1, & \text{если } gx_j = x_i, \\ 0, & \text{если } gx_j \neq x_i. \end{cases}$$

Поэтому $\chi(g) = \operatorname{Tr} A = \Big|\{i \mid gx_i = x_i\}\Big|$, что и требовалось доказать. □

Теперь применим это к регулярному представлению. Здесь и далее будем обозначать через $\rho = \rho_G$ характер регулярного представления конечной группы G.

Следствие 26.

$$\rho(g) = \begin{cases} |G|, & \text{если } g = 1, \\ 0, & \text{если } g \neq 1. \end{cases}$$

□

Теперь разложим регулярное представление на неприводимые. Пусть, как и прежде, $r_1, \ldots, r_m$ — система представителей классов эквивалентности неприводимых представлений группы G, $\chi_i = \chi_{r_i}$ — соответствующие неприводимые характеры, $d_i = \chi_i(1)$ — размерность представления r_i.

Предложение 27. *Регулярное представление изоморфно $d_1 r_1 \oplus \ldots \oplus d_m r_m$. В частности, $\rho = d_1\chi_1 + \ldots + d_m\chi_m$.*

Доказательство. Достаточно выразить характер ρ регулярного представления через неприводимые характеры. Если $\rho = k_1\chi_1 + \ldots + k_m\chi_m$, то $k_i = \langle \rho, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \rho(g)\overline{\chi_i(g)} = \overline{\chi_i(1)} = \chi_i(1) = d_i$, что и требовалось показать. □

Таким образом, все неприводимые представления входят в регулярное (с положительной кратностью), причем кратность вхождения равна размерности представления.

Следствие 28. $|G| = d_1^2 + \ldots + d_m^2$.

Доказательство. $|G| = \rho(1) = d_1\chi_1(1) + \ldots + d_m\chi_m(1) = d_1^2 + \ldots + d_m^2$. □

Теорема Веддерберна-Молина

Пусть G — конечная группа. Обозначим через $\mathrm{irrep}(G)$ число классов эквивалентности конечномерных неприводимых комплексных представлений группы G. Пусть $\mathrm{irrep}(G) = m$. Пусть $r_1, \ldots, r_m$ — система представителей классов эквивалентности конечномерных неприводимых комплексных представлений группы G, $\chi_i = \chi_{r_i}$ — соответствующие неприводимые характеры, $d_i = \chi_i(1)$ — размерность представления r_i.

Продолжим (по линейноти) представления $r_i : G \to GL(V_i) \simeq GL(d_i, \mathbb{C})$ до представлений групповой алгебры $\mathbb{C}G$, т.е. до гомоморфизмов алгебр $r_i : \mathbb{C}G \to \mathrm{End}(V_i) \simeq \mathrm{Mat}(d_i, \mathbb{C})$ (здесь $\mathrm{Mat}(n, \mathbb{C})$ — это алгебра всех квадратных матриц порядка n с комплексными матричными элементами; наши гомоморфизмы — это гомоморфизмы алгебр с единицей). Рассмотрим теперь гомоморфизм алгебр

$$F : \mathbb{C}G \to \mathrm{End}(V_1) \times \ldots \times \mathrm{End}(V_m) \simeq \mathrm{Mat}(d_1, \mathbb{C}) \times \ldots \times \mathrm{Mat}(d_m, \mathbb{C}),$$

заданный формулой $F(x) = (r_1(x), \ldots, r_m(x))$.

Теорема 29. (Веддерберн-Молин) *Гомоморфизм F является изоморфизмом, т.е.*

$$\mathbb{C}G \simeq \mathrm{Mat}(d_1, \mathbb{C}) \times \ldots \times \mathrm{Mat}(d_m, \mathbb{C}).$$

Доказательство. Проверим, что гомоморфизм F инъективен. В самом деле, $\mathrm{Ker}F = \cap_i \mathrm{Ker}r_i$. С другой стороны, рассмотрим регулярное представление алгебры $\mathbb{C}G$, т.е. $\Re : \mathbb{C}G \to \mathrm{End}\mathbb{C}G$, $\Re(x) : y \mapsto xy$. Это представление точное, т.е. $\mathrm{Ker}\Re = 0$. Но, как мы доказывали, $\Re \simeq d_1r_1 \oplus \ldots \oplus d_mr_m$ (т.е. существует изоморфизм линейных пространств $\varphi : \mathbb{C}G \to d_1V_1 \oplus \ldots \oplus d_mV_m$ такой, что $\Re(x) = \varphi^{-1}(d_1r_1 \oplus \ldots \oplus d_mr_m)(x)\varphi$ для всех $x \in \mathbb{C}G$. Отсюда следует, что $\mathrm{Ker}\Re = \cap_i \mathrm{Ker}r_i = \mathrm{Ker}F$, т.е. $\mathrm{Ker}F = 0$.

Далее остается сравнить размерности $\mathbb{C}G$ и $\mathrm{Mat}(d_1, \mathbb{C}) \times \ldots \times \mathrm{Mat}(d_m, \mathbb{C})$. В самом деле, $\dim \mathbb{C}G = |G| = d_1^2 + \ldots + d_m^2 = \dim(\mathrm{Mat}(d_1, \mathbb{C}) \times \ldots \times \mathrm{Mat}(d_m, \mathbb{C}))$, поэтому F — изоморфизм. □

Замечание. Классическая теорема Веддерберна гласит, что всякая полупростая конечномерная алгебра A над полем F изоморфна алгебре $\mathrm{Mat}(d_1, D_1) \times \ldots \times \mathrm{Mat}(d_m, D_m)$, где D_i — это коонечномерные тела над F. Если поле F алгебраически замкнуто, то на самом деле $A \simeq \mathrm{Mat}(d_1, F) \times \ldots \times \mathrm{Mat}(d_m, F)$ (ибо над F нет конечномерных тел, кроме самого F). Так как групповая алгебра $\mathbb{C}G$ полупроста, то мы в самом деле доказали сейчас для этого случая теорему Веддерберна.

Следствие 30. $\mathrm{irrep}(G) = \mathrm{cl}(G)$.

Доказательство. Рассмотрим снова изоморфизм Веддерберна-Молина

$$\mathbb{C}G \simeq \mathrm{Mat}(d_1, \mathbb{C}) \times \ldots \times \mathrm{Mat}(d_m, \mathbb{C}),$$

где $m = \mathrm{irrep}(G)$. Тогда

$$Z(\mathbb{C}G) \simeq Z(\mathrm{Mat}(d_1, \mathbb{C}) \times \ldots \times \mathrm{Mat}(d_m, \mathbb{C})) = Z(\mathrm{Mat}(d_1, \mathbb{C})) \times \ldots \times Z(\mathrm{Mat}(d_m, \mathbb{C})).$$

Поскольку центр полной матричной алгебры состоит из скалярных матриц, и потому одномерен (Упр. Проверьте, если Вы этого не знаете), то $\mathrm{cl}(G) = \dim Z(\mathbb{C}G) = \dim Z(\mathrm{Mat}(d_1, \mathbb{C})) \times \ldots \times Z(\mathrm{Mat}(d_m, \mathbb{C})) = m = \mathrm{irrep}(G)$. □

Следствие 31. *Неприводимые характеры образуют ортонормированный базис в* $Z(Fun(G), *)$.

Доказательство. Мы уже знаем, что неприводимые характеры образуют ортонормированную систему в $Z(\mathrm{Fun}(G), *)$. Остается заметить, что $\dim Z(\mathrm{Fun}(G), *) = \mathrm{cl}(G) = \mathrm{irrep}(G)$. □

Снова вернемся к изоморфизму Веддерберна-Молина

$$F : \mathbb{C}G \to \mathrm{Mat}(d_1, \mathbb{C}) \times \ldots \times \mathrm{Mat}(d_m, \mathbb{C}),$$

$F(x) = (r_1(x), \ldots, r_m(x))$. Пусть E_i — единица в алгебре $\mathrm{Mat}(d_i, \mathbb{C})$. Пусть e_i — ее прообраз в $\mathbb{C}G$ (точнее, $e_i = F^{-1}(0, \ldots, 0, E_i, 0, \ldots, 0)$). Тогда, очевидно, $1 = e_1 + \ldots + e_m$. Мы получили разложение единицы алгебры $\mathbb{C}G$ в сумму *центральных* (т.е. $e_i \in Z(\mathbb{C}G)$) *ортогональных* (т.е. $e_i e_j = 0$ при $i \neq j$) *идемпотентов* (т.е. $e_i^2 = e_i$). Нетрудно понять, что все (ненулевые) центральные идемпотенты в $\mathbb{C}G$ — это суммы нескольких e_i-х. В самом деле, $Z(\mathbb{C}G) \simeq Z(\mathrm{Mat}(d_1, \mathbb{C}) \times \ldots \times \mathrm{Mat}(d_m, \mathbb{C})) \simeq \mathbb{C} \times \ldots \times \mathbb{C}$, при этом e_i соответствует $(0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{C} \times \ldots \times \mathbb{C}$ (1 на i-м месте). Остается заметить, что $(a_1, \ldots, a_n) \in \mathbb{C} \times \ldots \times \mathbb{C}$ является идемпотентом тогда и только тогда, когда для каждого i имеем $a_i = 1$ или 0. В частности, идемпотенты e_i *неразложимы* (как центральные идемпотенты), т.е. не представимы в виде $u+v$, где u и v — (ненулевые) центральные идемпотенты (конечно, e_i могут быть разложимыми в классе всех идемпотентов).

Положим $U_i = (\mathbb{C}G)e_i = e_i(\mathbb{C}G)$. Заметим, что U_i — двусторонние идеалы в $\mathbb{C}G$; в частности, это подмодули (левого) регулярного модуля. Очевидно, $\mathbb{C}G = U_1 \oplus \ldots \oplus U_m$.

Предложение 32. U_i *— это изотипическая компонента регулярного* $\mathbb{C}G$*-модуля* $\mathbb{C}G$*, отвечающая неприводимому представлению* r_i.

Доказательство. Рассмотрим отображение $r_i : U_i \to \mathrm{Mat}(d_i, \mathbb{C})$. Это изоморфизм алгебр (с единицей; единица U_i — это e_i). Наделим $\mathrm{Mat}(d_i, \mathbb{C})$ структурой $\mathbb{C}G$-модуля "через r_i", т.е. $x \cdot A = r_i(x)A$, где $x \in \mathbb{C}G$, $A \in \mathrm{Mat}(d_i, \mathbb{C})$). Тогда r_i — изоморфизм $\mathbb{C}G$-модулей. Остается заметить, что $\mathbb{C}G$-модуль $\mathrm{Mat}(d_i, \mathbb{C})$ изоморфен сумме d_i экземпляров неприводимого $\mathbb{C}G$-модуля, отвечающего представлению r_i (достаточно разрезать матрицу на столбцы). □

Итак, мы установили естественное взаимно однозначное соответствие между неприводимыми представлениями группы G и неразложимыми центральными идемпотентами алгебры $\mathbb{C}G$.

Замечание. На языке идемпотентов разложение U_i в сумму d_i экземпляров неприводимого $\mathbb{C}G$-модуля, отвечающего представлению r_i, соответствует разложению e_i в сумму неразложимых ортогональных идемпотентов (конечно, уже не центральных). (И то, и другое разложение определено неоднозначно!) Именно, если $e_i = e_{i1} + \ldots + e_{id_i}$ — разложение в сумму неразложимых ортогональных идемпотентов, то $U_i = (\mathbb{C}G)e_{i1} \oplus \ldots \oplus (\mathbb{C}G)e_{id_i}$ (почему?), и $(\mathbb{C}G)e_{ij}$ — неприводимые модули. (Чтобы в этом убедиться, удобнее смотреть прямо на $\mathbb{C}G$-модуль $\mathrm{Mat}(d_i, \mathbb{C})$).

Нетрудно вычислить e_i в терминах неприводимых характеров.

Предложение 33.

$$e_i = \frac{d_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g.$$

Доказательство. Будем искать e_i в виде $e_i = \sum_{g \in G} a_i(g)g$. Так как $e_i \in Z(\mathbb{C}G)$, то $a_i \in Z(\mathrm{Fun}(G), *)$. По определению, $r_i(e_i) = E_i$, $r_j(e_i) = 0$ при $i \neq j$, т.е. $\chi_i(e_i) = d_i$, $\chi_j(e_i) = 0$ при $i \neq j$ (мы продолжаем характеры с G на $\mathbb{C}G$ по линейности). Поэтому $\sum_{g \in G} a_i(g)\chi_i(g) = d_i$, $\sum_{g \in G} a_j(g)\chi_i(g) = 0$ при $i \neq j$, т.е. $\langle \overline{a_i}, \chi_i \rangle = \frac{d_i}{|G|}$, $\langle \overline{a_i}, \chi_j \rangle = 0$ при $i \neq j$. Так как неприводимые характеры образуют ортонормированный базис в $Z(\mathrm{Fun}(G), *)$ (и $\overline{a_i} \in Z(\mathrm{Fun}(G), *)$), то $\overline{a_i} = \frac{d_i}{|G|}\chi_i$, т.е. $a_i = \frac{d_i}{|G|}\overline{\chi_i}$, что и требовалось доказать. □

Пусть $C_1, \ldots, C_m$ — все классы сопряженности в группе G, $c_i = C_i = \sum_{g \in C_i} g$. Мы построили два базиса в $Z(\mathbb{C}G)$: $e_1, \ldots, e_m$ и $c_1, \ldots, c_m$. Нетрудно найти матрицы перехода между этими базисами.

Зафиксируем (как угодно) $g_i \in C_i$ для каждого i. Тогда

$$e_j = \frac{d_j}{|G|} \sum_{g \in G} \overline{\chi_j(g)} g = \frac{d_j}{|G|} \sum_{i=1}^{m} \overline{\chi_j(g_i)} c_i.$$

Таким образом,

$$e_j = \sum_{i=1}^{m} x_{ij} c_i,$$

где

$$x_{ij} = \frac{d_j}{|G|} \overline{\chi_j(g_i)}.$$

Обратно, пусть

$$c_j = \sum_{i=1}^{m} y_{ij} e_i.$$

Тогда $\chi_i(c_j) = y_{ij}d_i$, т.е.

$$y_{ij} = \frac{1}{d_i}\chi_i(c_j) = \frac{|C_j|}{d_i}\chi_i(g_j).$$

Разумеется, матрицы $X = (x_{ij})$ и $Y = (y_{ij})$ взаимно обратны, т.е. $XY = YX = E$. Условие $YX = E$ — это в точности уже знакомая нам первая система соотношений ортогональности для характеров (Упр. Проверьте это.). А вот условие $XY = E$ дает нечто новое:

$$\sum_{k=1}^{m} x_{ik}y_{kj} = \frac{|C_j|}{|G|}\sum_{k=1}^{m}\overline{\chi_k(g_i)}\chi_k(g_j),$$

т.е.

$$\sum_{k=1}^{m}\chi_k(g_i)\overline{\chi_k(g_j)} = \begin{cases} \frac{|C_i|}{|G|} = |Z(G,g_i)|, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$$

Это и есть *вторая система соотношений ортогональности* для неприводимых характеров. Ее можно переписать и так:

Предложение 34.

$$\sum_{i=1}^{m}\chi_i(g)\overline{\chi_i(h)} = \begin{cases} |Z(G,g)|, & \text{если } g \text{ и } h \text{ сопряжены в } G, \\ 0, & \text{если } g \text{ и } h \text{ не сопряжены в } G. \end{cases}$$

□

Мы сталкиваемся с проявлениями двойственности между классами сопряженности группы и ее неприводимыми представлениями ("неабелев" аналог двойственности между G и $\widehat{G}$).

Примеры. Опишем неприводимые представления конкретных групп.

1. Пусть $G = S_3$, $|G| = 6$. Классы сопряженности: $C_1 = \{1\}$, $C_2 = \{\text{транспозиции}\}$, $C_3 = \{\text{циклы длины } 3\}$. Таким образом, $\mathrm{irrep}(G) = 3$. Так как $6 = d_1 + d_2 + d_3$, то $d_1 = d_2 = 1$, $d_3 = 2$ (с точностью до нумерации d_i-х). Одномерные представления — это 1 и sgn. Двумерный неприводимый модуль — это подмодуль, дополнительный к подмодулю констант в модуле $\mathrm{Fun}(X)$, где $X = \{1,2,3\}$ (G естественно действует на множестве X).

2. Пусть $G = S_4$, $|G| = 24$. Классы сопряженности: