Часть 1. Степени неприводимых представлений

Определение 1.1. Алгебраическое число $\alpha \in \overline{\mathbb{Q}}$ называется целым, если оно является корнем многочлена вида $x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$, где $a_1, \dots, a_n \in \mathbb{Z}$.

Лемма 1.2. *Алгебраическое число $\alpha \in \overline{\mathbb{Q}}$ — целое $\iff$ кольцо $\mathbb{Z}[\alpha] \subset \overline{\mathbb{Q}}$ — конечно порожденный $\mathbb{Z}$-модуль.*

Доказательство: $\Longrightarrow$) Если α — целое, то числа $1, \alpha, \dots, \alpha^{n-1}$ порождают $\mathbb{Z}[\alpha]$ как $\mathbb{Z}$-модуль.
$\Longleftarrow$) Пусть $\mathbb{Z}[\alpha]$ — конечно порожденный $\mathbb{Z}$-модуль, а $\alpha_1, \dots, \alpha_n$ — его образующие над $\mathbb{Z}$. Тогда имеем $\alpha\alpha_i = \sum_{j=1}^n a_{ij}\alpha_j$, где $A = (a_{ij})$ — целочисленная матрица. Заметим, что характеристический многочлен $\chi_A(x)$ матрицы A имеет целые коэффициенты. С другой стороны, по теореме Гамильтона–Кэли, имеем $\chi_A(A) = 0$. Но матрица A — это матрица умножения на α, следовательно, $\chi_A(\alpha) = 0$. $\square$

Замечание 1.3. Аналогично доказывается следующее утверждение. Если R — коммутативное кольцо, являющееся конечно порожденным $\mathbb{Z}$-модулем, то всякий элемент $\alpha \in R$ удовлетворяет полиномиальному уравнению вида $x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$, где $a_1, \dots, a_n \in \mathbb{Z}$.

Теорема 1.4. *Целые алгебраические числа образуют подкольцо в $\overline{\mathbb{Q}}$.*

Доказательство: нам надо проверить, что если α и β — целые, то $\alpha + \beta$ и $\alpha\beta$ — тоже целые. Рассмотрим подкольцо $\mathbb{Z}[\alpha, \beta] \subset \overline{\mathbb{Q}}$. Ясно, что оно является конечно порожденным $\mathbb{Z}$-модулем (набор элементов $(\alpha^i\beta^j)_{0\leqslant i\leqslant m-1, 0\leqslant j\leqslant n-1}$ при подходящих m и n порождает его). Следовательно, подкольца $\mathbb{Z}[\alpha+\beta] \subset \mathbb{Z}[\alpha, \beta]$ и $\mathbb{Z}[\alpha\beta] \subset \mathbb{Z}[\alpha, \beta]$ тоже являются конечно порожденными $\mathbb{Z}$-модулями. $\square$

Лемма 1.5. *Поле $\overline{\mathbb{Q}}$ является полем частных кольца целых алгебраических чисел.*

Доказательство: пусть $\alpha \in \overline{\mathbb{Q}}$ и $\mathrm{Irr}_\alpha^{\mathbb{Q}}(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$. Ясно, что $a_i \in \mathbb{Q}$ при всех i. Пусть m — НОК их знаменателей. Тогда многочлен $\mathrm{Irr}_{m\alpha}^{\mathbb{Q}}(x) = x^n + ma_1x^{n-1} + \dots + m^{n-1}a_{n-1}x + m^na_n$ имеет целые коэффициенты, значит $m\alpha$ — целое алгебраической число, а $\alpha = \frac{m\alpha}{m}$. $\square$

Лемма 1.6. *Рациональное число является целым алгебраическим $\iff$ оно целое.*

Доказательство: пусть $\alpha = r/s$ — корень многочлена $x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$. Тогда $r^n + a_1r^{n-1}s + \dots + a_{n-1}rs^{n-1} + a_ns^n = 0$. Можно считать, что r и s взаимно просты. Однако, если p — простой делитель числа s, то $p|r^n$, значит $p|r$. Следовательно, $s = \pm1$ и α — целое. $\square$

Лемма 1.7. *Если χ — характер представления конечной группы G над полем K характеристики 0, то $\chi(g)$ — целое алгебраическое число $\forall g \in G$.*

Доказательство: $\chi(g)$ — след оператора $\rho(g)$, то есть сумма его собственных значений (над полем $\overline{K}$). Однако, $\rho(g)^{|G|} = \rho(g^{|G|}) = \rho(1) = \mathrm{Id}$, поэтому все собственные значения являются корнями из единицы. В частности, они целые алгебраические числа. Следовательно и $\chi(g)$ — целое алгебраическое число. $\square$

Лемма 1.8. *Если V — неприводимое представление конечной группы G над полем $K = \overline{K}$, $\mathrm{char}\, K = 0$, а C — класс сопряженности то $\frac{1}{\dim V}\sum_{g\in C}\chi_V(g)$ — целое алгебраическое число.*

Доказательство: рассмотрим элемент $e_C := \sum_{g\in C} g \in K[G]$. Заметим, что e_C лежит в $Z(\mathbb{Z}[G])$ — центре целочисленного группового кольца. Однако, $Z(\mathbb{Z}[G])$ является $\mathbb{Z}$-подмодулем в $\mathbb{Z}[G]$, следовательно является $\mathbb{Z}$-модулем конечного типа. Значит, e_C удовлетворяет полиномиальному уравнению с целыми коэффициентами. Так как этому же уравению удовлетворяют и собственные числа оператора e_C в любом представлении группы G, то все они целые алгебраические числа. С другой стороны, так как e_C лежит в центре алгебры $K[G]$, то e_C действует в V умножением на некоторое число λ, причем $\lambda = \frac{\mathrm{Tr}\, e_C}{\dim V} = \frac{1}{\dim V}\sum_{g\in C}\chi_V(g)$. Остается заметить, что λ — собственное число для e_C. $\square$

Теорема 1.9. *Если V — неприводимое представление конечной группы G над полем $K = \overline{K}$, $\operatorname{char} K = 0$, то размерность V делит порядок G.*

Доказательство: $\frac{|G|}{\dim V} = \frac{1}{\dim V}\sum_{g\in G}\chi_V(g^{-1})\chi(g) = \sum_C \chi_V(g^{-1})\left(\frac{1}{\dim V}\sum_{g\in C}\chi(g)\right)$ — целое алгебраическое число. Однако, оно рациональное, значит оно целое. □

Часть 2. Ограничение и индукция

Пусть $\rho : G \to \mathrm{GL}(V)$ представление группы G, а $H \subset G$ – подгруппа. Тогда $\rho_{|H} : H \to \mathrm{GL}(V)$ — представление группы H, которое называется ограничением представления ρ на подгруппу H.

Лемма 2.1. *Ограничение является функтором из категории Rep_G в категорию Rep_H.*

Функтор ограничения обозначается Res_H^G.

Пусть теперь наоборот, $H \subset G$ – подгруппа, а U — представление группы H. Выберем представителей $1 = g_1, \dots, g_k$ в левых классах смежности G по H и рассмотрим пространство $K[G/H]$ с базисом $\{\, e_i \,\}_{i=1}^k$, занумерованном классами смежности. Далее, рассмотрим пространство $K[G/H]\otimes U = \bigoplus_{i=1}^k e_i \otimes U$ и введем в нем структуру G-модуля следующим образом. Для всякого $g \in G$ и $1 \leqslant i \leqslant k$ определим число $1 \leqslant s(g,i) \leqslant k$ как номер класса смежности элемента $g{\cdot}g_i \in G$, и определим элемент $h(g,i) \in H$ формулой $g{\cdot}g_i = g_{s(g,i)}{\cdot}h(g,i)$. Положим теперь $g(e_i \otimes u) = e_{s(g,i)} \otimes h(g,i)u$.

Ясно, что $s(g'g,i) = s(g', s(g,i))$, $h(g'g,i) = h(g', s(g,i))h(g,i)$. Отсюда сразу следует, что $K[G/H]\otimes U$ — представление группы G. Более того, ясно, что $s(h,1) = 1$, $h(h,1) = h$, поэтому естественное вложение $f_U : U \to K[G/H]\otimes U$, $u \mapsto e_1 \otimes u$, является морфизмом H-модулей. Покажем, что оно обладает следующим универсальным свойством:

> *если V — представление группы G, а $f : U \to V$ — морфизм H-модулей, то существует единственный морфизм G-модулей $\tilde f : K[G/H]\otimes U \to V$, такой что $\tilde f \circ f_U = f$.*

Действительно, если $\tilde f$ — такой морфизм, то $\tilde f(e_i \otimes u) = \tilde f(g_i(e_1 \otimes u)) = g_i \tilde f(f_U(u)) = g_i f(u)$, поэтому $\tilde f$ — единственный. С другой стороны, определяя $\tilde f$ формулой $\tilde f(\sum e_i \otimes u_i) = \sum g_i f(u_i)$, получаем морфизм G-модулей: $\tilde f(g\sum e_i \otimes u_i) = \tilde f(\sum e_{s(g,i)} \otimes h(g,i)u_i) = \sum g_{s(g,i)} f(h(g,i)u_i) = \sum g_{s(g,i)} h(g,i) f(u_i) = \sum (g\cdot g_i) f(u_i) = g\sum g_i f(u_i) = g\tilde f(\sum e_i \otimes u_i)$.

Построенное нами представление группы G называется представлением, индуцированным с представления U группы H, и обозначается $\mathrm{Ind}_H^G(U)$, а доказанное нами универсальное свойство может быть переформулировано следующим образом:

Теорема 2.2. *Если U и V — представления групп H и G, то $\mathrm{Hom}_H(U, \mathrm{Res}_H^G(V)) = \mathrm{Hom}_G(\mathrm{Ind}_H^G(U), V)$.*

Следствие 2.3. *Индуцированное представление не зависит от выбора представителей классов сопряженности.*

Пример 2.4. Легко видеть, что $\mathrm{Ind}_{\{1\}}^G K \cong K[G]$ — представление группы G, индуцированное с тривиального представления единичной подгруппы является регулярным представлением. Обобщением этого примера является изоморфизм $\mathrm{Ind}_H^G K[H] \cong K[G]$.

Следствие 2.5. *Индукция является функтором из категории Rep_H в категорию Rep_G.*

Доказательство: пусть $f : U \to U'$ — морфизм H-модулей. Определим $\mathrm{Ind}_H^G(f)$ как морфизм G-модулей $\mathrm{Ind}_H^G U \to \mathrm{Ind}_H^G U'$, соответствующий композиции $U \xrightarrow{f} U' \xrightarrow{f_{U'}} \mathrm{Res}_H^G \mathrm{Ind}_H^G(U')$. □

Замечание 2.6. Свойство $\mathrm{Hom}_H(U, \mathrm{Res}_H^G(V)) = \mathrm{Hom}_G(\mathrm{Ind}_H^G(U), V)$ называется сопряженностью этих функторов. Оно аналогично свойству сопряженности операторов относительно билинейной формы. Пары сопряженных функторов часто встречаются в математике. Например, функтор $\mathcal{S}ets \to \mathcal{G}r$, сопоставляющий множеству порожденную им свободную группу, сопряжен к забывающему структуру группы функтору $\mathcal{G}r \to \mathcal{S}ets$.

Лемма 2.7. *Имеем* $\chi_{\mathrm{Ind}_H^G U}(g) = \dfrac{1}{|H|} \sum\limits_{\substack{s\in G\\ s^{-1}gs\in H}} \chi_U(s^{-1}gs)$.

Доказательство: выберем базис $\{ u_j \}$ в пространстве U и рассмотрим базис $\{ e_i \otimes u_j \}$ пространства $\mathrm{Ind}_H^G U$. Ясно, что матрица оператора g в этом базисе является блочно-перестановочной, соответствующей перестановке $i \mapsto s(g,i)$. Значит ее след равен сумме следов блоков, таких что $s(g,i) = i$, то есть $g \cdot g_i = g_i \cdot h$, то есть $g_i^{-1} \cdot g \cdot g_i \in H$. Значит, $\chi(g) = \sum_{i \ | \ g_i^{-1}gg_i\in H} \chi_U(g_i^{-1}gg_i)$. Заметим, теперь, что если $s = g_i h$, то $s^{-1}gs = h^{-1}g_i^{-1}gg_ih$. В частности, $s^{-1}gs \in H \iff g_i^{-1}gg_i \in H$, причем $\chi_U(s^{-1}gs) = \chi_U(g_i^{-1}gg_i)$, откуда и получаем искомую формулу. □

Замечание 2.8. Поведение характера при ограничении еще проще. Легко видеть, что $\chi_{\mathrm{Res}_H^G V}(h) = \chi_V(h)$.

Индукция помогает строить представления.

Пример 2.9. Пусть $G = \mathfrak{S}_3$, $H = A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Рассмотрим любое нетривиальное линейное представление группы H. Вычисляя характер, видим, что индуцированное представление является неприводимым двумерным представлением группы $\mathfrak{S}_3$.

Часть 3. Дополнения

Пусть $G = G_1 \times G_2$, а V_1 и V_2 — представления групп G_1 и G_2 соответственно. В тензорном произведении $V_1 \otimes V_2$ зададим структуру представления группы G формулой $(g_1,g_2)(v_1\otimes v_2) = (g_1v_1)\otimes(g_2v_2)$.

Лемма 3.1. *Пусть V_1 и V_1' — неприводимые G_1-модули, а V_2 и V_2' — неприводимые G_2-модули.*
(i) $V_1 \otimes V_2 \cong V_1' \otimes V_2' \iff V_1 \cong V_1'$, $V_2 \cong V_2'$. (ii) Если $\overline{K} = K$, то $V_1 \otimes V_2$ неприводимо над $G_1 \times G_2$.

Доказательство: заметим, что $\chi_{V_1\otimes V_2}(g_1,g_2) = \chi_{V_1}(g_1)\chi_{V_2}(g_2)$.

(i) Имеем очевидное равенство $\langle \chi_{V_1\otimes V_2}, \chi_{V_1'\otimes V_2'}\rangle = \frac{1}{|G_1\times G_2|}\sum_{(g_1,g_2)\in G_1\times G_2} \chi_{V_1}(g_1^{-1})\chi_{V_2}(g_2^{-1})\chi_{V_1'}(g_1)\chi_{V_2'}(g_2) = \left(\frac{1}{|G_1|}\sum_{g_1\in G_1}\chi_{V_1}(g_1^{-1})\chi_{V_1'}(g_1)\right)\left(\frac{1}{|G_2|}\sum_{g_2\in G_2}\chi_{V_2}(g_2^{-1})\chi_{V_2'}(g_2)\right) = \langle\chi_{V_1},\chi_{V_1'}\rangle\langle\chi_{V_2},\chi_{V_2'}\rangle$. Если теперь при $i = 1$ или $i = 2$ имеем $V_i \ncong V_i'$, то $\langle \chi_{V_i}, \chi_{V_i'}\rangle = 0$, значит $\langle \chi_{V_1\otimes V_2}, \chi_{V_1'\otimes V_2'}\rangle = 0$ и $V_1\otimes V_2 \ncong V_1'\otimes V_2'$.

(ii) Предыдущее равенство показывает, что $\langle \chi_{V_1\otimes V_2}, \chi_{V_1\otimes V_2}\rangle = \langle\chi_{V_1},\chi_{V_1}\rangle\langle\chi_{V_2},\chi_{V_2}\rangle = 1$. □

Замечание 3.2. Над незамкнутым полем утверждение (ii) предыдущей леммы вообще говоря неверно. Например, если $K = \mathbb{R}$, $G_1 = \mathbb{Z}/3\mathbb{Z}$, $G_2 = \mathbb{Z}/5\mathbb{Z}$, а V_1 и V_2 — двумерные неприводимые представления.

Лемма 3.3. *Имеем изоморфизм $(G_1 \times G_2)$-модулей $K[G_1\times G_2] \cong K[G_1]\otimes K[G_2]$.*

Доказательство: отображение $e_{(g_1,g_2)} \mapsto e_{g_1}\otimes e_{g_2}$ является искомым изоморфизмом. □

Теорема 3.4. *Если $\overline{K} = K$, то всякое неприводимое представление группы $G_1\times G_2$ однозначно представляется в виде $V_1\otimes V_2$, где V_1 и V_2 — неприводимые представления групп G_1 и G_2.*

Доказательство: нам осталось проверить, что всякое неприводимое представление группы $G_1 \otimes G_2$ имеет указанный вид. Действительно, $K[G_1\times G_2] = K[G_1]\otimes K[G_2] = (\oplus V_{1,i})\otimes(\oplus V_{2,j}) = \oplus(V_{1,i}\otimes V_{2,j})$.

Еще одно доказательство получается, если вычислить сумму квадратов размерностей представлений вида $V_{1,i}\otimes V_{2,j}$: имеем $\sum_{i,j}(d_{1,i}d_{2,j})^2 = (\sum_i d_{1,i}^2)(\sum_j d_{2,j}^2) = |G_1||G_2| = |G_1\times G_2|$. □

Замечание 3.5. Над незамкнутым полем утверждение теоремы вообще говоря неверно. Можно утверждать лишь то, что всякое неприводимое представление группы $G_1 \times G_2$ является прямым слагаемым в представлении вида $V_1 \otimes V_2$.