Независимый Московский Университет

Алгебра – II

Второй курс, осенний семестр 1999/2000 г.
Лекции 8,9

Полупростые алгебры и представления конечных групп. Пусть A — алгебра над полем $\Bbbk$ (напомню, что мы всегда предполагаем A ассоциативной конечномерной алгеброй с единицей). Для каждого $a \in A$ рассмотрим следующие операторы в A как в линейном пространстве над $\Bbbk$: оператор $L(a)$ левого умножения на a и оператор $R(a)$ правого умножения на a. Мы получаем две алгебры линейных операторов в пространстве A: алгебру $L(A)$ операторов вида $L(a)$ (действующих слева) и алгебру $R(A)$ операторов вида $R(a)$ (действующих справа).

Утверждение 1. *Каждая из алгебр $L(A)$ и $R(A)$ изоморфна алгебре A. Кроме того, $\mathrm{End}_{L(A)} A = R(A)$ и $\mathrm{End}_{R(A)} A = L(A)$.*

Доказательство. Рассмотрим естественный гомоморфизм $A \to L(A)$, переводящий $a \in A$ в $L(a)$. Ясно, что он сюръективен. Пусть a_0 принадлежит его ядру. Тогда $a_0 = a_0 \cdot 1 = L(a_0)1 = 0$. Поэтому $L(A) \simeq A$. Аналогично, $R(A) \simeq A$.

Пусть теперь $\varphi \in \mathrm{End}_{L(A)} A$. Положим $b = 1\varphi$. Тогда $a\varphi = (L(a)1)\varphi = L(a)(1\varphi) = ab = aR(b)$ для любого $a \in A$, то есть $\varphi = R(b)$. Поэтому $\mathrm{End}_{L(A)} A = R(A)$. Аналогично доказываем, что $\mathrm{End}_{R(A)} A = L(A)$. $\square$

Определение 1. Алгебра A называется *полупростой*, если она полупроста как левый модуль над собой.

Теорема 2. *Полупростая алгебра A над алгебраически замкнутым полем $\Bbbk$ изоморфна прямой сумме матричных алгебр над этим полем.*

Доказательство. Разложим A как левый A-модуль в прямую сумму простых модулей, собирая вместе изоморфные слагаемые:

$$A \simeq W = \underbrace{V_1 \oplus \cdots \oplus V_1}_{n_1} \oplus \cdots \oplus \underbrace{V_k \oplus \cdots \oplus V_k}_{n_k},$$

где $V_1, \ldots, V_k$ — неизоморфные простые левые A-модули. Пусть $n = n_1 + \cdots + n_k$ Любой элемент $w \in W$ записывается в виде $w = (v_1, \ldots, v_n)$, где $v_i \in V_1$ при $1 \leqslant i \leqslant n_1$, $v_i \in V_2$ при $n_1 + 1 \leqslant i \leqslant n_1 + n_2$, и т. д.

Рассмотрим произвольный A-эндоморфизм $F : W \to W$. Применим его к элементу вида

$$w_i(v) = (0, \ldots, 0, v, 0, \ldots, 0),$$

где $v \in V_r$ стоит на i-м месте. Получим

$$w_i(v)F = (vF_{i1}, \ldots, vF_{in}),$$

где, очевидно, $F_{ij} \in \mathrm{Hom}_A(V_r, V_s)$ (гомоморфизмы A-модулей мы пишем справа; номер s простого A-модуля V_s определяется индексом j). Поскольку любой ненулевой гомоморфизм между простыми A-модулями является изоморфизмом, то $F_{ij} = 0$ при $r \neq s$, а при $r = s$ по лемме Шура F_{ij} — умножение на некоторую константу $\lambda_{ij} \in \Bbbk$. Поэтому применение эндоморфизма F к строке $(u_1, \dots, u_n)$ — это умножение ее справа на блочно-диагональную матрицу (λ_{ij}) с размерами блоков $n_1, \dots, n_k$. Таким образом, $\mathrm{End}_A W = M_{n_1}(\Bbbk) \oplus \dots \oplus M_{n_k}(\Bbbk)$. Однако $\mathrm{End}_A W \simeq \mathrm{End}_{L(A)} A = R(A) \simeq A$ по утверждению 1. □

Отметим, что из полученного описания алгебры A следует, что $\dim V_i = n_i$, и что A-модуль V_i изоморфен $\Bbbk^{n_i}$ со следующим действием алгебры A: для $a \in A$ находим образ A при выбранном изоморфизме $A \xrightarrow{\sim} M_{n_1}(\Bbbk) \oplus \dots \oplus M_{n_k}(\Bbbk)$, выделяем i-й диагональный блок (размером $n_i \times n_i$), и применяем эту матрицу к элементам $\Bbbk^{n_i}$.

Теорема 3. *Пусть алгебра A полупроста и $V_1, \dots, V_k$ — все неизоморфные простые A-модули, входящие в разложение A как левого A-модуля. Тогда любой левый A-модуль полупрост, и любой простой левый A-модуль изоморфен одному из V_i.*

Доказательство. Подмодуль A как левого A-модуля — это не что иное, как левый идеал. Представим A как прямую сумму минимальных (ненулевых) левых идеалов: $A = \bigoplus I_j$, где, по предположению, каждый из идеалов I_j изоморфен (как левый A-модуль) некоторому из V_i. Пусть V — произвольный левый A-модуль, и пусть $v \in V$. Тогда $Av = \sum I_j v$, где каждый из подмодулей $I_j v$ либо простой (изоморфный одному из V_i), либо нулевой. Пусть $(v_1, \dots, v_s)$ — базис V. Тогда $V = \sum A v_r = \sum I_j v_r$, то есть модуль V является суммой простых модулей. Следовательно, он полупрост. Если он прост, то равен одному из слагаемых $I_j v_r$, поэтому изоморфен одному из V_i. □

Чтобы применять полученные теоремы к представлениям конечной группы, мы должны найти некоторую алгебру, теория представлений которой будет эквивалентна теории представлений группы.

Определение 2. Для конечной группы G рассмотрим линейное пространство $\Bbbk G$ всех формальных линейных комбинаций элементов группы. На базисе пространства $\Bbbk G$ определено ассоциативное умножение (групповая операция); распространяя её по дистрибутивности на всё пространство $\Bbbk G$, получаем на нём структуру ассоциативной алгебры с единицей. Эта алгебра называется *групповой алгеброй* группы G.

Пусть V — конечномерное векторное пространство над полем $\Bbbk$, и $\rho : G \to \mathrm{End}_{\Bbbk} V$ — линейное представление группы G. Определим в пространстве V операцию левого умножения на элементы групповой алгебры, положив $\Big(\sum\limits_{g \in G} \lambda_g g\Big) v = \sum\limits_{g \in G} \lambda_g \rho(g) v$.

Упражнение 1. Доказать, что таким образом пространство V приобретает структуру левого $\Bbbk G$-модуля. Более того, предъявленная конструкция $\Bbbk G$-модуля по представлению группы G продолжается до функтора из категории конечномерных линейных представлений группы G над полем $\Bbbk$ в категорию конечномерных левых $\Bbbk G$-модулей, осуществляющего эквивалентность этих категорий.

Теорема 4 (Машке). *Пусть G — конечная группа, $\Bbbk$ — поле, причем $\operatorname{char}\Bbbk$ не делит $|G|$. Тогда любой конечномерный $\Bbbk G$-модуль полупрост.*

Доказательство. Пусть V — конечномерный $\Bbbk G$-модуль, и U — его подмодуль. Рассмотрим произвольное линейное отображение $\pi_0 : V \to U$, тождественное на U (проекцию вдоль некоторого дополнительного подпространства W_0). Положим

$$\pi v = \frac{1}{|G|} \sum_{g \in G} g \pi_0 g^{-1} v$$

для любого $v \in V$. Отображение $\pi : V \to U$ тоже линейно, тождественно на U, но ещё и G-*инвариантно*, то есть $h\pi = \pi h$ для любого $h \in G$. Поэтому $W = \operatorname{Ker}\pi$ является $\Bbbk G$-помодулем модуля V. При этом $V = U \oplus W$. □

Следствие 4.1. *При $\operatorname{char}\Bbbk$ не делящей $|G|$ групповая алгебра $\Bbbk G$ полупроста.*

Итак, мы можем применить теоремы 2 и 3 к групповой алгебре конечной группы. При этом, зная о существовании разложения алгебры в прямую сумму матричных колец, мы не знаем самого этого разложения. Поэтому важно выразить как можно больше свойств этого разложения в инвариантных терминах.

Прежде всего, размерность алгебры A выражается через числа n_i по формуле $\dim A = \sum n_i^2$. Поэтому из теоремы 3 следует

Утверждение 5. *Размерность полупростой алгебры A над алгебраически замкнутым полем равна сумме квадратов размерностей неизоморфных простых A-модулей.*

Следствие 5.1. *Пусть поле $\Bbbk$ алгебраически замкнуто и его характеристика не делит порядок конечной группы G. Тогда сумма квадратов размерностей неэквивалентных неприводимых представлений группы G над полем $\Bbbk$ равна порядку этой группы.*

Дадим теперь важное

Определение 3. *Центром* алгебры A называется множество всех таких элементов $z \in A$, что $za = az$ для любого $a \in A$. Центр алгебры A обозначается через $Z(A)$.

Центр ассоциативной алгебры с единицей является коммутативной алгеброй с единицей.

Ясно, что центр полной матричной алгебры состоит только из скалярных матриц. Кроме того, центром прямой суммы алгебр является прямая сумма центров слагаемых. Поэтому размерность центра равна числу слагаемых. Отсюда получаем

Утверждение 6. *Число неизоморфных простых A-модулей для полупростой алгебры A над алгебраически замкнутым полем равно* $\dim Z(A)$.

Пусть $A = \Bbbk G$. Найдем $Z(A)$. Ясно, что $z = \sum\limits_{g \in G} \lambda_g g$ принадлежит $Z(A)$ тогда и только тогда, когда $hz = zh$ для любого $h \in G$. Поэтому

$$Z(A) = \Big\{ \sum_{g \in G} \lambda_g g \;\Big|\; (\forall g, h \in G)\ \lambda_{h^{-1}gh} = \lambda_g \Big\}.$$

Отсюда следует, что размерность центра групповой алгебры равна числу классов сопряженных элементов. Итак, получается

Следствие 6.1. *Пусть поле $\Bbbk$ алгебраически замкнуто и его характеристика не делит порядок конечной группы G. Тогда число неэквивалентных неприводимых представлений группы G над полем $\Bbbk$ равно числу классов сопряженных элементов этой группы.*

Теория характеров.

Определение 4. Пусть A — ассоциативная алгебра, а V — левый A-модуль. На двойственном пространстве V^* можно ввести структуру *правого* A-модуля, положив $(\xi a)(v) = \xi(av)$ для любых $\xi \in V^*$ и $v \in V$. Полученный правый A-модуль V^* называется *двойственным модулем* к V.

Определение 5. Пусть V — левый A-модуль, а U — правый A-модуль. Билинейная форма $B : U \times V \to \Bbbk$ называется *A-инвариантной*, если $B(ua, v) = B(u, av)$ для любых $u \in U$, $v \in V$ и $a \in A$.

Упражнение 2. Доказать, что билинейная форма $B : U \times V \to \Bbbk$ является A-инвариантной тогда и только тогда, когда соответствующее линейное отображение $U \to V^*$ является гомоморфизмом правых A-модулей (и тогда и только тогда, когда соответствующее линейное отображение $V \to U^*$ является гомоморфизмом левых A-модулей).

Пусть A — ассоциативная алгебра над полем $\mathbb{C}$ (или любым алгебраически замкнутым полем характеристики ноль). Рассмотрим билинейную форму $(a, b) = \operatorname{tr} L_a L_b$ на A (напомню, что для любого $a \in A$ через L_a мы обозначаем оператор левого умножения на a в алгебре A).

Упражнение 3. Доказать, что эта билинейная форма является симметрической и A-инвариантной.

Утверждение 7. *Пусть алгебра A полупроста. Тогда билинейная форма $(\ ,\ )$ невырождена.*

Доказательство. По теореме 2 существует разложение $A = \bigoplus A_i$, где A_i — идеал, изоморфный $M_{n_i}(\mathbb{C})$. Идеалы A_i попарно ортогональны относительно формы (,) (докажите это!). Поэтому достаточно проверить невырожденность ограничения нашей формы на каждый из идеалов A_i, другими словами, надо доказать утверждение в случае $A = M_n(\mathbb{C})$.

Однако для $a, b \in M_n(\mathbb{C})$ мы имеем $\operatorname{tr} L_a L_b = \operatorname{tr} L_{ab} = n \operatorname{tr} ab$ (докажите это!). Поэтому невырожденность формы (,) следует из невырожденности формы $\operatorname{tr} ab$ на $M_n(\mathbb{C})$. □

Итак, для полупростой алгебры над полем $\mathbb{C}$ форма (,) определяет изоморфизм A как левого и правого A-модуля с двойственным модулем A^*. Если $A = \mathbb{C}G$, то A^* естественно отождествляется с пространством $\mathbb{C}[G]$ комплексных функций на группе. Посмотрим, какой вид имеет форма (,) на $\mathbb{C}G$ и соответствующий изоморфизм $\mathbb{C}G \to \mathbb{C}[G]$.

Заметим, что для любого неединичного $g \in G$ у матрицы оператора L_g на главной диагонали стоят нули, т. е. $\operatorname{tr} L_g = 0$. Если же $g = e$, то $L_g = \mathrm{id}$ и $\operatorname{tr} L_g = |G|$. Отсюда мы получаем, что

$$\Big(\sum_{g\in G} \lambda_g g, \sum_{g\in G} \mu_g g\Big) = |G| \sum_{g\in G} \lambda_g \mu_{g^{-1}}.$$

Соответствующий изоморфизм $\mathbb{C}G \to \mathbb{C}[G]$ переводит g в $|G|^{-1}\delta_{g^{-1},\bullet}$ — функцию на G, равную $|G|^{-1}$ на g^{-1} и нулю на остальных элементах группы G. Перенося с помощью этого изоморфизма билинейную форму (,) с $\mathbb{C}G$ на $\mathbb{C}[G]$, получаем

$$(f_1, f_2) = |G|^{-1} \sum_{g\in G} f_1(g) f_2(g^{-1}).$$

Определение 6. Пусть ρ — представление группы G в конечномерном векторном пространстве V над полем $\Bbbk$. *Характером* представления ρ называется функция $\chi_\rho(g) = \operatorname{tr} \rho(g) \in \Bbbk[G]$. характер неприводимого представления называется *неприводимым характером* группы G.

Теорема 8. *Пусть $V_1, \ldots, V_k$ — все неизоморфные простые $\mathbb{C}G$-модули, $n_i = \dim V_i$, а $\chi_1, \ldots, \chi_k$ — характеры соответствующих представлений группы G. Положим*

$$\varepsilon_i = \frac{n_i}{|G|} \sum_{g\in G} \chi_i(g) g^{-1} \in \mathbb{C}G.$$

Тогда элементы ε_i принадлежат центру алгебры $\mathbb{C}G$, составляют его базис и, кроме того, удовлетворяют соотношениям:

1) $\varepsilon_i^2 = \varepsilon_i$;
2) $\varepsilon_i \varepsilon_j = 0$ *при* $i \neq j$;
3) $\sum_{i=1}^{k} \varepsilon_i = 1$.

Доказательство. Обозначим через ρ_i представление группы G в пространстве V_i. Той же буквой мы будем обозначать представление алгебры $\mathbb{C}G$ в пространстве V_i. Характер $\chi_i \in \mathbb{C}[G]$ мы рассматриваем как линейную функцию на $\mathbb{C}G$, пользуясь отождествлением $(\mathbb{C}G)^* = \mathbb{C}[G]$. Ясно, что $\chi_i(x) = \operatorname{tr}\rho_i(x)$ для любого $x \in \mathbb{C}G$.

Мы знаем, что алгебра $\mathbb{C}G$ изоморфна алгебре $A = \bigoplus_{i=1}^{k} M_{n_i}(\mathbb{C})$. Пусть $\psi : A \to \mathbb{C}G$ — изоморфизм. Естественный базис центра алгебры A составляют элементы вида $E_i = (0, \ldots, 0, E, \ldots, 0)$, где единичная матрица стоит на i-м месте, а на остальных — нули. Докажем, что $\psi(E_i) = \varepsilon_i$.

Представление $\rho_i \circ \psi$ алгебры A эквивалентно представлению в пространстве $\mathbb{C}^{n_i}$, где каждый элемент $a = (a_1, \ldots, a_k)$ действует матрицей $a_i \in M_{n_i}(\mathbb{C})$. Поэтому $\operatorname{tr}\rho_i \circ \psi(a) = \operatorname{tr} a_i$. С другой стороны, $\operatorname{tr} L_a L_{E_i} = \operatorname{tr} L_{aE_i} = n_i \operatorname{tr} a_i$. Поэтому $(x, \psi(E_i)) = n_i\chi_i(x) = (x, \varepsilon_i)$ для любого $x \in \mathbb{C}G$. Из невырожденности формы $(\ ,\ )$ следует, что $\psi(E_i) = \varepsilon_i$.

Итак, элементы $(\varepsilon_1, \ldots, \varepsilon_k) = (\psi(E_1), \ldots, \psi(E_k))$ — базис $Z(\mathbb{C}G)$. Соотношения между ними следуют из соответствующих соотношений между E_i, которые очевидны. □

Замечание. Из доказательства теоремы ясно, что ε_i действует единичным оператором в V_i и нулем во всех остальных простых $\mathbb{C}G$-модулях V_j. Поэтому в произвольном $\mathbb{C}G$-модуле ε_i действует как инвариантный проектор на *i-ю изотипическую компоненту*, то есть на сумму всех простых $\mathbb{C}G$-подмодулей, изоморфных V_i.

Следствие 8.1. *Характеры различных неприводимых комплексных представлений группы G линейно независимы и составляют базис пространства функций на G, постоянных на классах сопряженных элементов.*

Доказательство. Характер χ_i — образ $n_i^{-1}\varepsilon_i$ при изоморфизме $\mathbb{C}G \xrightarrow{\sim} \mathbb{C}[G]$, задаваемом формой $(\ ,\ )$. Поскольку ε_i составляют базис в $Z(\mathbb{C}G)$, то и χ_i составляют базис в образе этого пространства, равном, как легко видеть, пространству функций на G, постоянных на классах сопряженных элементов. □

Следствие 8.2. *Для неприводимых комплексных характеров χ_i группы G выполнено следующее соотношенее ортогональности:*

$$(\chi_i, \chi_j) = \delta_{ij}.$$

Доказательство. Это следует из очевидного равенства $(\varepsilon_i, \varepsilon_j) = n_i^2$. □

Следствие 8.3. *Характер χ комплексного представления группы G является неприводимым тогда и только тогда, когда $(\chi, \chi) = 1$.*

Доказательство. Это следует из того, что характер прямой суммы представлений равен сумме их характеров, а любое комплексное представление группы G является вполне приводимым. □

Упражнение 4. Пусть V, W — $\mathbb{C}G$-модули, а χ_V, χ_W — соответствующие характеры. Доказать, что $\dim \operatorname{Hom}_G(V, W) = (\chi_V, \chi_W)$.

Утверждение 9. *Пусть χ — характер комплексного представления ρ группы G в пространстве V. Тогда $\chi(g^{-1}) = \overline{\chi(g)}$ для любого $g \in G$.*

Доказательство. В любом $\mathbb{C}G$-модуле есть G-инвариантное эрмитово скалярное произведение (действительно, можно взять любое эрмитово скалярное произведение и усреднить его по группе G, как мы это делали с проектором в доказательстве теоремы Машке). Выберем такое скалярное произведение в пространстве V и запишем матрицы операторов представления в какой-нибудь ортонормированном базисе. Пусть $C(g)$ — матрица оператора $\rho(g)$. Тогда $C(g^{-1}) = C(g)^{-1} = \overline{C(g)^t}$. Поэтому $\chi(g^{-1}) = \overline{\chi(g)}$. □

Следствие 9.1. *Определим в $\mathbb{C}[G]$ эрмитово скалярное произведение $\langle\ ,\ \rangle$ формулой*

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

Тогда для любых двух характеров χ_1, χ_2 выполнено равенство

$$\langle \chi_1, \chi_2\rangle = (\chi_1, \chi_2)$$

В силу этого соотношение ортогональности для характеров и его следствия остаются справедливыми при замене билинейной формы $(\ ,\ )$ на эрмитову форму $\langle\ ,\ \rangle$.

Утверждение 10. *Характеры комплексных представлений конечной группы принимают только целые алгебраические значения.*

Доказательство. Пусть G — конечная группа, $\rho : G \to \operatorname{End}_{\mathbb{C}} V$ — ее представление и $\chi(g) = \operatorname{tr}\rho(g)$ — характер этого представления. Обозначим через m порядок группы G. Каждое собственное значение оператора $\rho(g)$ является корнем m-й степени из единицы, то есть целым алгебраическим числом (для любого $g \in G$). Поэтому и след $\rho(g)$ является целым алгебраическим числом. □

Теорема 11. *Размерность любого неприводимого комплексного представления конечной группы делит порядок группы.*

Доказательство. Пусть G — конечная группа, V — простой $\mathbb{C}G$-модуль, χ — характер соответствующего неприводимого представления и $n = \dim V$. Мы знаем, что элемент

$$\varepsilon = \frac{n}{|G|}\sum_{g\in G}\chi(g)g^{-1} \in \mathbb{C}G$$

действует в пространстве V единичным оператором. Положим $\mathcal{A} = \frac{|G|}{n}\varepsilon$. Тогда

$$\operatorname{tr}\mathcal{A}^k = \sum_{g_1,\dots,g_k\in G}\chi(g_1)\dots\chi(g_k)\chi(g_1^{-1}\cdot g_k^{-1}).$$

Из этой формулы видно, что $\operatorname{tr}\mathcal{A}^k$ выражается в виде многочлена с целыми коэффициентами от значений характера χ и, следовательно, является целым алгебраическим числом. С другой стороны, $\operatorname{tr}\mathcal{A}^k = \frac{|G|^k}{n^{k-1}}$ — рациональное число. Из целозамкнутости $\mathbb{Z}$ следует, что $\frac{|G|^k}{n^{k-1}}$ — число целое. Поскольку это верно для любого натурального k, мы получаем, что $\frac{|G|}{n}$ — целое число. $\square$

Теорема 12. *Любой неодномерный неприводимый комплексный характер конечной группы равен нулю хотя бы на одном классе сопряженности.*

Доказательство. Предположим, что неприводимый характер χ конечной группы G не принимает нулевого значения. Обозначим соответствующее неприводимое представление через ρ, а его размерность — через n. Рассмотрим произвольный элемент $g \in G$. Пусть ω — некоторый примитивный корень степени $|G|$ из 1. Тогда, очевидно, любое собственное значение оператора $\rho(g)$ имеет вид ω^k для некоторого целого k, а значение характера χ на g можно записать как $\chi(g) = \omega^{k_1} + \dots + \omega^{k_n}$, где $k_1, \dots, k_n \in \mathbb{Z}$. При этом $\overline{\chi(g)} = \omega^{-k_1} + \dots + \omega^{-k_n}$. Отсюда следует, что для любого вложения $\varphi : \mathbb{Q}(\omega) \to \mathbb{C}$ имеет место равенство $\varphi(\overline{\chi(g)}) = \overline{\varphi(\chi(g))}$, поскольку при любом вложении ω должен переходить в некоторый примитивный корень степени $|G|$ из 1.

Согласно соотношению ортогональности,

$$\sum_{g \in G} \chi(g)\overline{\chi(g)} = |G|. \tag{1}$$

Применим к тождеству (1) всевозможные вложения $\varphi : \mathbb{Q}(\omega) \to \mathbb{C}$ и составим среднее арифметическое полученных равенств:

$$\sum_{g \in G} \Big(\frac{1}{r} \sum_{\varphi \in \Phi} \varphi\big(\chi(g)\overline{\chi(g)}\big) \Big) = |G|,$$

где через Φ обозначено множество всех вложений поля $\mathbb{Q}(\omega)$ в поле комплексных чисел и $r = |\Phi|$. Поскольку

$$\varphi\big(\chi(g)\overline{\chi(g)}\big) = \varphi(\chi(g))\varphi(\overline{\chi(g)}) = \varphi(\chi(g))\overline{\varphi(\chi(g))} = |\varphi(\chi(g))|^2 > 0,$$

мы можем применить неравенство среднего арифметического и среднего геометрического:

$$\sum_{g \in G} \sqrt[r]{\prod_{\varphi \in \Phi} \varphi\big(\chi(g)\overline{\chi(g)}\big)} \leqslant |G|,$$

Заметим, что средним геометрическим чисел $\varphi\big(\chi(g)\overline{\chi(g)}\big)$ является корень степени r из нормы целого алгебраического числа $\chi(g)\overline{\chi(g)}$. Норма целого алгебраического числа — целое число, а среднее геометрическое положительных чисел — число положительное, поэтому для каждого $g \in G$ среднее геометрическое всех чисел $\varphi\big(\chi(g)\overline{\chi(g)}\big)$ не меньше единицы. Однако сумма всех этих средних геометрических не больше числа слагаемых. Поэтому каждое из слагаемых равно единице. В частности, норма $|\chi(e)|^2$, где e — единица группы G, равна 1. Однако $\chi(e) = n$. Поэтому $n = 1$. $\square$