§5. Представления Галуа

5.1. Теорема Крулля – Шмидта. Пусть A — ассоциативная (но не обязательно коммутативная) алгебра[1] над произвольным полем $\Bbbk$, а V — левый модуль над нею, т. е. векторное пространство над $\Bbbk$ с таким билинейным левым действием $A \times V \to V$, $(a, v) \mapsto av$, что $(ab)v = a(bv)$ и $1v = v$ для всех $v \in V$ и $a, b \in A$. Иначе можно сказать, что отображение $\lambda\colon A \to \mathrm{End}_{\Bbbk}(V)$, $a \mapsto (\lambda_a\colon v \mapsto av)$ является гомоморфизм $\Bbbk$-алгебр. В дальнейшем нас будут интересовать только групповые алгебры $A = \Bbbk G \overset{\text{def}}{=} \{\sum_{g\in G} x_g g \mid x_g \in \Bbbk\}$ конечных групп G с коэффициентами в поле $\Bbbk$. Такая алгебра представляет собой векторное пространство над $\Bbbk$ с базисом G, и умножение в ней билинейно продолжает операцию композиции на группе G:

$$\Big(\sum_g x_g g\Big)\Big(\sum_h y_h h\Big) \overset{\text{def}}{=} \sum\nolimits_{gh} x_g y_h gh = \sum_f z_f f\,,\ \text{где } z_f = \sum_{gh=f} x_g y_h\,. \tag{5-1}$$

A-модуль V называется *разложимым*, если $V = U \oplus W$, где $U, W \subsetneq V$ — собственные ненулевые A-подмодули. Очевидно, что всякий конечномерный как векторное пространство над $\Bbbk$ модуль V является прямой суммой неразложимых. Такое разложение обычно далеко не единственно: например, если $A = \Bbbk[t]$ и t действует на V тождественным оператором, то любое разложение пространства V в прямую сумму одномерных подпространств является разложением в прямую сумму неразложимых A-подмодулей. Тем не менее, *теорема Крулля – Шмидта*, которую мы докажем в этом разделе, утверждает, что прямые слагаемые любых двух разложений можно биективно сопоставить друг другу так, что соответственные слагаемые будут изоморфны[2]. В частности, для любого неразложимого A-модуля U и произвольного A-модуля V корректно определена *кратность* $m_U(V)$ вхождения U в V, равная количеству изоморфных модулю U слагаемых в любом разложении модуля V в прямую сумму неразложимых модулей, и A-модули V и W изоморфны, если и только если $m_U(V) = m_U(W)$ для всех неразложимых A-модулей U.

Мы будем называть $\Bbbk$-линейное отображение $\varphi\colon V \to W$ между A-модулями *A-линейным* (или *гомоморфизмом A-модулей*), если $\varphi(av) = a\varphi(v)$ для всех $a \in A$ и $v \in V$. Такие отображения образуют ассоциативную $\Bbbk$-подалгебру $\mathrm{Hom}_A(V, W) \subset \mathrm{Hom}_{\Bbbk}(V, W)$.

Лемма 5.1 (лемма Фиттинга)
Для всякого эндоморфизма $\varphi \in \mathrm{End}_A(V)$ любого конечномерного A-модуля V существует разложение $V = U \oplus N$ в прямую сумму таких φ-инвариантных A-подмодулей, один из которых может оказаться нулевым, что ограничение $\varphi|_U$ биективно, а ограничение $\varphi|_N$ нильпотентно.

Доказательство. Так как цепочки $V \supseteq \operatorname{im}\varphi \supseteq \operatorname{im}\varphi^2 \supseteq \dots$ и $0 \subseteq \ker\varphi \subseteq \ker\varphi^2 \subseteq \dots$ в какой-то момент стабилизируются, найдётся такое $m \in \mathbb{N}$, что $\operatorname{im}\varphi^n = \operatorname{im}\varphi^m$ и $\ker\varphi^n = \ker\varphi^m$ при всех $n > m$. Положим $U = \operatorname{im}\varphi^m$, $N = \ker\varphi^m$. Оба подпространства являются φ-инвариантными

[1] См. раздел 5.2 на с. 90 лекций [Алг 1].

[2] Теорема Крулля-Шмидта справедлива для ассоциативной алгебры A над произвольным коммутативным кольцом с единицей и любого A-модуля V, в котором всякая возрастающая и всякая убывающая цепочка вложенных подмодулей стабилизируются через конечное число шагов (первое условие называется *нётеровостью*, второе — *артиновостью* модуля V). Более того, она обобщается на пучки модулей над пучками алгебр и на неабелевы группы с действием множества операторов A. Поскольку нам эта теорема понадобится только для конечномерных модулей над групповой алгеброй группы Галуа, мы докажем её для конечномерных модулей, однако все шаги этого доказательства достаточно прямолинейно переносятся и на более общие случаи.

A-подмодулями, и ограничение $\varphi|_N$ нильпотентно, ибо $\ker(\varphi^m|_{\ker\varphi^m}) = \ker\varphi^{2m} = \ker\varphi^m$, а ограничение $\varphi|_U$ сюръективно, поскольку сюръективно ограничение $\varphi^m|_U$:

$$\operatorname{im}(\varphi^m|_{\operatorname{im}\varphi^m}) = \operatorname{im}\varphi^{2m} = \operatorname{im}\varphi^m .$$

В силу конечномерности U ограничение $\varphi|_U$ биективно. Поэтому $U \cap N = 0$. Наконец, $V = (\varphi^m)^{-1}(\varphi^m(V)) = (\varphi^m)^{-1}(\varphi^m\varphi^m(V)) = \varphi^m(V) + \ker\varphi^m = U + N$. □

Следствие 5.1
Каждый A-линейный эндоморфизм конечномерного неразложимого A-модуля либо биективен, либо нильпотентен. □

Следствие 5.2
Если сумма $\varphi_1 + \ldots + \varphi_n$ эндоморфизмов конечномерного неразложимого A-модуля биективна, то биективно хотя бы одно из её слагаемых.

Доказательство. Индукция по количеству слагаемых сводит всё к случаю $n = 2$. Пусть эндоморфизм $\sigma = \varphi_1 + \varphi_2$ биективен. Положим $\psi_i = \sigma^{-1}\varphi_i$. Тогда $\psi_1 + \psi_2 = \mathrm{Id}_V$, и по предыдущему сл. 5.1 каждый из эндоморфизмов ψ_i либо биективен, либо нильпотентен. Если ψ_1 биективен, то $\varphi_1 = \sigma\psi_1$ тоже биективен. Если ψ_1 нильпотентен, то $\psi_1(v) = 0$ для некоторого $v \neq 0$, и так как $v = \psi_1(v) + \psi_2(v) = \psi_2(v)$, мы заключаем, что $\psi_2^m(v) = v \neq 0$ для всех m. Тем самым ψ_2 не нильпотентен, а значит биективен. Но тогда биективен и $\varphi_2 = \sigma\psi_2$. □

Лемма 5.2 (лемма о замене)
Пусть конечномерный A-модуль V имеет два разложения $U \oplus W = V = S_1 \oplus \ldots \oplus S_m$, в которых U и все S_i неразложимы. Тогда $U \simeq S_i$ и $V = S_i \oplus W$ для некоторого i.

Доказательство. Обозначим через $\pi_U, \pi_i \in \mathrm{End}_A(V)$ проекторы модуля V на подмодули U и S_i соответственно вдоль подмодулей W и $W_i \stackrel{\text{def}}{=} \bigoplus_{\nu\neq i} S_\nu$. Тогда $\sum_i \pi_i = \mathrm{Id}_V$, откуда

$$\mathrm{Id}_U = \pi_U|_U = \pi_U\big(\sum_i \pi_i\big)\big|_U = \sum_i \pi_U\pi_i|_U ,$$

и по сл. 5.2 хотя бы одна из композиций

$$\pi_U\pi_i|_U : U \to U \tag{5-2}$$

биективна. Пусть $U' = \pi_i(U)$. Поскольку композиция (5-2) инъективна, сюръекция

$$\pi_i|_U : U \twoheadrightarrow U'$$

имеет нулевое ядро, а значит, задаёт изоморфизм $U \xrightarrow{\sim} U'$. По той же причине

$$U' \cap W = \pi_i(U) \cap \ker\pi_U = 0 .$$

Так как $\dim U' + \dim W = \dim U + \dim W = \dim V$, мы заключаем, что $V = U' \oplus W$. С другой стороны, $U' = \pi_i(U) \subset S_i$, и в силу биективности композиции (5-2) ограничение $\pi_U|_{S_i} : S_i \to U$ является сюръекцией, изоморфно отображающей U' на U. Поэтому $S_i = U' \oplus \ker(\pi_U|_{S_i})$. В силу неразложимости модуля S_i он совпадает с U'. □

Следствие 5.3 (теорема Крулля – Шмидта)
Если конечномерные A-модули $U_1, \dots, U_n$ и $W_1, \dots, W_m$ неразложимы, то $\bigoplus_i U \simeq \bigoplus_j W_j$ тогда и только тогда, когда $m = n$ и после надлежащей перенумерации $U_i \simeq W_i$ при всех i.

Доказательство. Можно считать, что $U_1 \oplus \dots \oplus U_n = V = W_1 \oplus \dots \oplus W_m$ являются разложениями одного и того же A модуля V. Применяя предыдущую лем. 5.2 к $U = U_1$, $W = \bigoplus_{\nu>1} U_\nu$ и $S_i = W_i$, заключаем, что после надлежащей перенумерации модулей W_i мы можем считать, что $U_1 \simeq W_1$ и $W_1 \oplus U_2 \oplus \dots \oplus U_n = V = W_1 \oplus W_2 \oplus \dots \oplus W_m$. Тогда $U_2 \oplus \dots \oplus U_n \simeq V/W_1 \simeq W_2 \oplus \dots \oplus W_m$, и мы можем повторить предыдущее рассуждение. Так как размерность модуля на каждом шагу строго уменьшается, процесс через конечное число шагов закончится. □

Следствие 5.4
Наличие изоморфизма $W_1 \oplus V \simeq W_2 \oplus V$ для конечномерных A-модулей V, W_1, W_2 равносильно наличию изоморфизма $W_1 \simeq W_2$.

Доказательство. Из теоремы Крулля – Шмидта вытекает, что кратность вхождения неразложимого A-модуля U в прямую сумму модулей аддитивна:

$$m_U(W_1 \oplus V) = m_U(W_1) + m_U(V) \quad \text{и} \quad m_U(W_2 \oplus U) = m_U(W_2) + m_U(V)\,.$$

Поэтому равенства $m_U(W_1) = m_U(W_2)$ и $m_U(W_1 \oplus V) = m_U(W_2 \oplus U)$ эквивалентны друг другу для всех неразложимых U. □

Следствие 5.5
Обозначим через $W^{\oplus n}$ прямую сумму n копий модуля W. Наличие изоморфизма $W_1^{\oplus n} \simeq W_2^{\oplus n}$ для конечномерных A-модулей W_1, W_2 равносильно наличию изоморфизма $W_1 \simeq W_2$.

Доказательство. Так как $m_U(W_1^{\oplus n}) = n m_U(W_1)$ и $m_U(W_2^{\oplus n}) = n m_U(W_2)$ для любого неразложимого A-модуля U, равенства $m_U(W_1) = m_U(W_2)$ и $m_U(W_1^{\oplus n}) = m_U(W_2^{\oplus n})$ эквивалентны. □

5.2. Теорема о нормальном базисе. Пусть $\mathbb{F} \supset \Bbbk$ — конечное расширение Галуа с группой Галуа $G = \operatorname{Gal} \mathbb{F}/\Bbbk$. Поле $\mathbb{F}$ является конечномерным левым модулем над групповой алгеброй $\Bbbk G$. В этом разделе мы покажем, что это свободный модуль ранга 1, т. е. существует такой элемент $\vartheta \in \mathbb{F}$, что каждый $\xi \in \mathbb{F}$ однозначно представляется в виде

$$\xi = \sum_{g \in G} x_g\, g(\vartheta)\,, \text{ где } x_g \in \Bbbk\,.$$

Другими словами, Галуа-орбита элемента ϑ является базисом поля $\mathbb{F}$ как векторного пространства над $\Bbbk$. Такой базис $\mathbb{F}$ над $\Bbbk$ называется *нормальным*, и факт его существования известен как *теорема о нормальном базисе*. Остаток этого раздела посвящён её доказательству.

Расширим[1] векторное пространство $\mathbb{F}$ над полем $\Bbbk$ до векторного пространства $W = \mathbb{F} \otimes_\Bbbk \mathbb{F}$ над полем $\mathbb{F}$. Константы $\lambda \in \mathbb{F}$ действуют на разложимые тензоры $w = \mu \otimes_\Bbbk \zeta \in W$ по правилу

[1] Из всякого векторного пространства V над полем $\Bbbk$ можно изготовить векторное пространство $W = \mathbb{F} \otimes_\Bbbk V$ над полем $\mathbb{F}$. Умножение на скаляры из $\mathbb{F}$ задаётся на разложимых тензорах правилом $\lambda \cdot (\mu \otimes \nu) \stackrel{\text{def}}{=} (\lambda\mu) \otimes \nu$, которое корректно продолжается по линейности на всё W. Эта операция называется *расширением скаляров* с $\Bbbk$ до $\mathbb{F}$. Примером расширения скаляров является комплексификация вещественных векторных пространств, см. раздел 15.2 на с. 243 лекций [Алг 1]. Например, комплексификация $\mathbb{C} \otimes_\mathbb{R} \mathbb{C}$ самого поля $\mathbb{C}$, рассматриваемого как двумерное векторное пространство над $\mathbb{R}$.

$\lambda w = (\lambda\mu)\otimes_{\Bbbk}\zeta$, а каждый $\Bbbk$-линейный оператор $g\colon \mathbb{F}\to\mathbb{F}$ из группы G продолжается до $\mathbb{F}$-линейного оператора $\mathrm{Id}_F\otimes_{\Bbbk} g\colon W\to W$, $\mu\otimes_{\Bbbk}\zeta\mapsto\mu\otimes_{\Bbbk} g(\zeta)$, который мы по прежнему будем обозначать буквой g. Таким образом, пространство W является левым модулем над групповой алгеброй $\mathbb{F}G$ группы G с коэффициентами в поле $\mathbb{F}$. Покажем, что это свободный модуль ранга 1. Для этого рассмотрим двойственное пространство $W^* = \mathrm{Hom}_{\mathbb{F}}(W,\mathbb{F})$.

Упражнение 5.1. Убедитесь, что $\dim_{\mathbb{F}} W = \dim_{\mathbb{F}} W^* = [\mathbb{F}:\Bbbk]$.

Пусть $n = [\mathbb{F}:\Bbbk] = |G|$. Каждый элемент $g\in G$ задаёт $\mathbb{F}$-линейную форму $x_g\in W^*$,

$$x_g\colon W\to\mathbb{F},\ \mu\otimes\zeta\mapsto\mu g(\zeta).$$

Эти формы обладают свойством $x_g(hw) = x_{gh}(w)$ для всех $g,h\in G$ и $w\in W$ и линейно независимы над $\mathbb{F}$, поскольку вычисляя обе части равенства $\sum_{g\in G}\lambda_g x_g = 0$, где $\lambda_g\in\mathbb{F}$, на векторе $1\otimes\zeta\in W$, получаем для всех $\zeta\in\mathbb{F}$ равенство $\sum_{g\in G}\lambda_g g(\zeta) = 0$, возможное только когда все $\lambda_g = 0$, так как функции $g\colon \mathbb{F}^\times\to\mathbb{F}^\times$ являются различными мультипликативными характерами мультипликативной группы $\mathbb{F}^\times$ со значениями в поле $\mathbb{F}$ и, стало быть, линейно независимы в пространстве функций $\mathbb{F}^\times\to\mathbb{F}$ по упр. 4.9 на стр. 40. Мы заключаем, что n линейных форм x_g образуют базис n-мерного пространства W^* над $\mathbb{F}$. Поэтому $\mathbb{F}$-линейное отображение

$$\Phi\colon W\to\mathbb{F}G,\ w\mapsto\sum_{g\in G} x_{g^{-1}}(w)\cdot g,$$

инъективно, а в силу равенства размерностей левой и правой части и биективно. Поскольку отображение Φ перестановочно с действием элементов $h\in G$:

$$\Phi(hw) = \sum_{g\in G} x_{g^{-1}}(hw)\cdot g = \sum_{g\in G} x_{g^{-1}h}(w)\cdot g = \sum_{\substack{s\in G\\(s=h^{-1}g)}} x_{s^{-1}}(w)\cdot hs = h\Phi(w)$$

оно является изоморфизмом $\mathbb{F}G$-модулей.

Пусть элементы $f_1,\dots,f_n$ образуют базис поля $\mathbb{F}$ как векторного пространства над $\Bbbk$. Для каждого i множество $f_i\Bbbk G = \{\sum_{g\in G} f_i y_g g \mid y_g\in\Bbbk\}\subset\mathbb{F}G$ является $\Bbbk G$-подмодулем в $\mathbb{F}G$, изоморфным $\Bbbk G$, и $\mathbb{F}G = \bigoplus_i f_i\Bbbk G$. Мы заключаем, что пространство $W\simeq\mathbb{F}G$ как модуль над групповой алгеброй $\Bbbk G$ изоморфно $(\Bbbk G)^{\oplus n}$.

С другой стороны, подпространства $f_i\otimes_{\Bbbk}\mathbb{F}\subset\mathbb{F}\otimes_{\Bbbk}\mathbb{F} = W$ тоже являются $\Bbbk G$-подмодулями в W, и каждый из них изоморфен $\Bbbk G$-модулю $\mathbb{F}$, а $W = \bigoplus_i f_i\otimes_{\Bbbk}\mathbb{F}$. Таким образом, $W\simeq\mathbb{F}^{\oplus n}$ как левый $\Bbbk G$-модуль. В силу сл. 5.5 на стр. 47 наличие изоморфизмов $\Bbbk G$-модулей

$$\mathbb{F}^{\oplus n}\simeq W\simeq(\Bbbk G)^{\oplus n}$$

влечёт наличие изоморфизма $\Bbbk G$-модулей $\mathbb{F}\simeq\Bbbk G$, что и доказывает теорему о нормальном базисе.

5.3. Когомологии $H^0(G,A)$ и $H^1(G,A)$ и теорема 90 Гильберта. Пусть G — произвольная группа. Абелева группа A называется G-модулем, если задано действие группы G на A групповыми автоморфизмами. Результат применения автоморфизма $g\in G$ к элементу $a\in A$ мы обозначаем через $ga\in A$. Подгруппа

$$A^G \stackrel{\text{def}}{=} \{a\in A\mid ga = a\ \forall\, g\in G\},$$

на которой G действует тривиально, называется *подмодулем G-инвариантов*. Если заданы G-модули A и B, то мы обозначаем через

$$\mathrm{Hom}_G(A,B) = \{\varphi\colon A\to B,\mid \varphi(ga) = g\varphi(a)\}$$

подгруппу инвариантов действия группы G на абелевой группе гомоморфизмов $\operatorname{Hom}(A,B)$ по правилу $g:\ \varphi \mapsto g\varphi g^{-1}$ и называем G-инвариантные гомоморфизмы *G-гомоморфизмами* или *гомоморфизмами G-модулей*. Каждая точная тройка[1] G-модулей

$$0 \to A \to B \to C \to 0\,,$$

все стрелки в которой являются G-гомоморфизмами, порождает точную последовательность модулей G-инвариантов

$$0 \to A^G \to B^G \to C^G\,,$$

правая стрелка в которой не обязательно сюръективна в силу того, что G-инвариантность класса $[b]_A \in C = B/A$, т. е. равенство $g[b]_A - [b]_A = [0]_A$ для всех $g \in G$, означает всего лишь то, что $gb - b \in A$ для всех $g \in G$. Таким образом, выбор определённого представителя $b \in B$ в классе $c \in C$ задаёт отображение

$$\delta_b:\ G \to A\,,\ g \mapsto gb - b\,, \tag{5-3}$$

и у класса $c \in C^G$ тогда и только тогда имеется прообраз в B^G, когда существует такой представитель $b \in B$ класса $c \in C$, для которого отображение (5-3) тождественно нулевое. При выборе другого представителя $b' = b + a$ в том же классе c получится отображение

$$\delta_{b+a} = \delta_b + \delta_a:\ g \mapsto gb + ga - b - a\,. \tag{5-4}$$

Мы заключаем, что класс $c \in C^G$ поднимается в B^G, если и только если $\delta_b = \delta_a$ для некоторого представителя $b \in B$ в классе $c \in C$ и некоторого $a \in A$.

Отображение (5-3) обладает замечательным свойством (обязательно убедитесь в этом!):

$$\delta_b(gh) = \delta_b(g) + g\delta_b(h)\,,$$

которое можно интерпретировать как вырождение правила Лейбница. А именно, пусть абелева группа W является одновременно и левым и правым[2] G-модулем, причём левое и правое действия G на W коммутируют друг с другом[3]. Отображение $\psi:\ G \to W$ называется *дифференцированием* группы G со значениями в *бимодуле* W, если оно удовлетворяет *правилу Лейбница*:

$$\psi(gh) = \psi(g)h + g\psi(h) \quad \forall\, g,h \in G\,. \tag{5-5}$$

Упражнение 5.2. Покажите, что каждое дифференцирование зануляется на единице группы.

Всякий левый G-модуль A можно превратить в бимодуль, снабдив его тривиальным правым действием G, т. е. полагая $ag = a$ для всех $a \in A$ и $g \in G$. Тогда правило Лейбница (5-5) редуцируется в свойство

$$\psi(gh) = \psi(g) + g\psi(h) \quad \forall\, g,h \in G\,. \tag{5-6}$$

---

[1] Цепочка гомоморфизмов абелевых групп $\dots \xrightarrow{\alpha} C \xrightarrow{\beta} \dots$ называется *точной* в C, если $\ker\beta = \operatorname{im}\alpha$. Точность цепочки гомоморфизмов $0 \to A \to B \to C \to 0$ в каждом месте означает, что $A \subset B$ является подгруппой в B и $C = B/A$. Такие точные цепочки называются *точными тройками*, см. листок $6\frac{1}{2}$ прошлогоднего курса «Алгебра-1».

[2] Т. е. имеется такое правое умножение $W \times G \to W$, $(w,g) \mapsto wg$, что $(w_1 + w_2)g = w_1 g + w_2 g$, $w(gh) = (wg)h$ и $w \cdot 1 = w$ для всех $w, w_1, w_2 \in W$ и $g \in G$. Иначе можно сказать, что отображение $G \to \operatorname{Aut} W$, $g \mapsto (w \mapsto wg)$ является *антигомоморфизмом* групп (оборачивает порядок сомножителей).

[3] Т. е. $(gw)h = g(wh)$ для всех $w \in W$ и $g,h \in G$. Такие W называются *G-бимодулями*.

Обладающие этим свойством отображения $\psi\colon G \to A$ называются *дифференцированиями* группы G со значениями в *левом G-модуле A* или *скрещенными гомоморфизмами* из G в A.

Упражнение 5.3. Убедитесь, что дифференцирования образуют подгруппу в абелевой группе G^A всех отображений $G \to A$.

Эта подгруппа обозначается $\mathrm{Der}(G, A)$. Выше мы видели, что для любого $a \in A$ отображение $\delta_a\colon g \mapsto ga - a$ является дифференцированием. Такие дифференцирования называются *главными*. Из формулы (5-4) вытекает, что $\delta_{a\pm b} = \delta_a \pm \delta_b$. Поэтому главные дифференцирования образуют подргуппу $\mathrm{PrDer}(G, A) \subset \mathrm{Der}(G, A)$.

Определение 5.1 (группы когомологий $H^0(G, A)$ и $H^1(G, A)$)
Для любого (левого) G-модуля A группы

$$H^0(G, A) \stackrel{\text{def}}{=} A^G \quad \text{и} \quad H^1(G, A) \stackrel{\text{def}}{=} \mathrm{Der}(G, A)/\mathrm{PrDer}(G, A)$$

называются *нулевой* и *первой* группами *когомологий* группы G с коэффициентами в A.

Предложение 5.1
Каждая точная тройка $0 \to A \to B \to C \to 0$ левых G-модулей производит точную последовательность когомологий

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \xrightarrow{\delta} H^1(G, A) \xrightarrow{\alpha} H^1(G, B) \xrightarrow{\beta} H^1(G, C)\,, \tag{5-7}$$

в которой гомоморфизм δ сопоставляет классу $[b] \in C^G$ класс дифференцирования (5-3):

$$\delta_b\colon G \to A\,,\ g \mapsto gb - b\,,$$

по модулю подгруппы $\mathrm{PrDer}(G, A)$ главных дифференцирований, гомоморфизм α сопоставляет дифференцированию $\psi\colon G \to A$ его композицию с вложением $A \hookrightarrow B$, а гомоморфизм β сопоставляет дифференцированию $\varphi\colon G \to B$ его композицию с эпиморфизмом $B \twoheadrightarrow C = B/A$ факторизации по подгруппе $A \subset B$.

Доказательство. Из формулы (5-4) вытекает, что отображение δ корректно определено[1] и является гомоморфизмом абелевых групп. Как мы видели выше, G-инвариантный класс $c \in C^G$ является образом G-инвариантного класса $b \in B^G$, если и только если $\delta_b \in \mathrm{PrDer}(G, A)$. Это доказывает точность последовательности (5-7) в $H^0(G, C)$. Корректность определения гомоморфизмов α и β и оставшейся точности является несложным упражнением. □

Упражнение 5.4. Убедитесь, что композиция любого дифференцирования $\psi\colon G \to V$ с произвольным гомоморфизмом G-модулей $\varphi\colon V \to W$ является дифференцированием группы G со значениями в G-модуле W, и проверьте точность последовательности (5-7) в $H^1(G, A)$ и в $H^1(G, B)$.

[1] Т. е. при выборе другого представителя $b' = b + a$ в том же классе $c = [b] = [b'] \in C = B/A$ дифференцирование $\delta_{b'} = \delta_b + \delta_a$ остаётся в том же классе по модулю главных дифференцирований $\delta_a\colon G \to A$.

Пример 5.1 (когомологии циклической группы)
Пусть $G = C_n$ — циклическая группа порядка n, порождённая элементом g. Тогда любое дифференцирование $\psi\colon C_n \to A$ со значениями в произвольном C_n-модуле A однозначно определяется своим значением на элементе g, так как по (вырожденному) правилу Лейбница

$$\begin{aligned}\psi(g^k) = \psi(g\cdot g^{k-1}) = \psi(g) + g\psi(g^{k-1}) = \psi(g) + g\cdot\psi(g^{k-1}) + g^2\psi(g^{k-2}) = \ldots = \\ = \psi(g) + g\psi(g) + g^2\psi(g) + \ldots + g^{k-1}\psi(g)\,.\end{aligned}$$

Поскольку $\psi(g^n) = \psi(e) = 0$ по упр. 5.2 на стр. 49, элемент $a = \psi(g) \in A$ удовлетворяет соотношению

$$\sum_{h\in C_n} h(a) = a + g(a) + \ldots + g^{n-1}(a) = 0\,. \tag{5-8}$$

Наоборот, для любого удовлетворяющего этому соотношению элемента $a \in A$ отображение

$$\psi_a\colon C_n \to A\,,\ g^k \mapsto \sum_{\nu=0}^{k-1} g^\nu(a)$$

является дифференцированием группы C_n со значениями в A.

Упражнение 5.5. Убедитесь в этом.

Таким образом, группа $\mathrm{Der}(C_n, A)$ изоморфна группе решений линейного уравнения (5-8) в группе A. Главные дифференцирования $\delta_a\colon g \mapsto g(a) - a$ отвечают таким решениям уравнения (5-8), которые попадают в образ эндоморфизма $g - \mathrm{Id}_A\colon A \to A$. Левая часть уравнения (5-8) является результатом применения к элементу $a \in A$ *норменного эндоморфизма*

$$N\colon A \to A\,,\ a \mapsto \sum_{h\in C_n} h(a)\,. \tag{5-9}$$

Мы заключаем, что $H^1(C_n, A) \simeq \ker N / \mathrm{im}(g - \mathrm{Id}_A)$. К примеру, для $C_n = C_2 = \{\pm 1\}$ и C_2-модуля $A = \mathbb{Z}/(n)$, на котором образующая $-1 \in C_2$ действует умножением на -1, получаем $\ker N = A$, а $\mathrm{im}(g - e) = 2A \subset A$ равен A при нечётном n и является подгруппой индекса 2 при чётном n. Тем самым

$$H^1(C_2, \mathbb{Z}/(n)) = \begin{cases} \mathbb{Z}/(2) & \text{при чётном } n \\ 0 & \text{при нечётном } n\,, \end{cases}$$

и это согласуется с тем, что последовательность инвариантных относительно смены знака подгрупп в точной последовательности групп $\mathbb{Z}/(2) \hookrightarrow \mathbb{Z}/(4) \twoheadrightarrow \mathbb{Z}/(2)$, левая стрелка которой переводит $[1]_2$ в $[2]_4$, не является точной[1].

Упражнение 5.6. Обозначим через $\mathbb{Z}C_n$ групповую алгебру группы C_n с целыми коэффициентами. Докажите, что бесконечная последовательность гомоморфизмов абелевых групп

$$0 \leftarrow \mathbb{Z} \xleftarrow{\varepsilon} \mathbb{Z}C_n \xleftarrow{g-e} \mathbb{Z}C_n \xleftarrow{N} \mathbb{Z}C_n \xleftarrow{g-e} \mathbb{Z}C_n \xleftarrow{N} \ldots\,,$$

в которой стрелки, помеченные как $g - e$ и N, суть операторы умножения на $g - e$ и N соответственно, а $\varepsilon\colon \mathbb{Z}C_n \to \mathbb{Z}$, $\sum_{h\in C_n} z_h h \mapsto \sum_{h\in C_n} z_h$, всюду точна.

[1] Она имеет вид $\mathbb{Z}/(2) \xrightarrow{\simeq} \mathbb{Z}/(2) \xrightarrow{0} \mathbb{Z}/(2)$ с нулевой правой стрелкой.

Пример 5.2 (аддитивная теорема Э. Нётер)
Пусть $\mathbb{F} \supset \Bbbk$ — конечное расширение Галуа с группой Галуа $G = \operatorname{Gal} \mathbb{F}/\Bbbk$. Покажем, что

$$H^1(G, \mathbb{F}) = \operatorname{Der}(G, \mathbb{F})/\operatorname{PrDer}(G, \mathbb{F}) = 0\,.$$

Для любого дифференцирования $\psi\colon G \to \mathbb{F}$, $g \mapsto \psi_g$, числа $\psi_h \in \mathbb{F}$ связаны равенствами

$$\psi_{hg} = \psi_h + h(\psi_g) \quad \forall\, g, h \in G\,, \tag{5-10}$$

которые начале прошлого века принято было называть *аддитивными уравнениями Нётер*[1]. Главное дифференцирование $\delta_\zeta\colon G \to \mathbb{F}^\times$ имеет $\psi_h = h(\zeta) - \zeta$. По теореме о нормальном базисе существует элемент $\vartheta \in \mathbb{F}$, Галуа образы которого $g(\vartheta)$, $g \in G$, образуют базис $\mathbb{F}$ как векторного пространства над $\Bbbk$. Сумма $\sigma = \sum_{g\in G} g(\vartheta)$ этих базисных векторов отлична от нуля и инвариантна относительно группы Галуа. Для произвольного решения $\psi = \{\psi_h \in \mathbb{F}^\times \mid h \in G\}$ уравнений (5-11) положим $\zeta = \sum_{g\in G} \psi_g \cdot g(\vartheta)$. Тогда для всех $h \in G$

$$h(\zeta) = \sum_{g\in G} h(\psi_g) \cdot hg(\vartheta) = \sum_{g\in G} (\psi_{hg} - \psi_h) \cdot hg(\vartheta) = \zeta - \psi_h \cdot \sigma\,,$$

откуда $\psi_h = (h(\zeta) - \zeta)/\sigma = h(\zeta/\sigma) - (\zeta/\sigma)$, т. е. $\psi = \delta_{\zeta/\sigma}$ является главным дифференцированием.

Пример 5.3 (мультипликативная теорема Э. Нётер[2])
В условиях предыдущего примера мультипликативная абелева группа $\mathbb{F}^\times$ поля $\mathbb{F}$ тоже является G-модулем. В мультипликативных обозначениях дифференцирование группы G со значениями в $\mathbb{F}^\times$ — это такое отображение $\psi\colon G \to \mathbb{F}^\times$, $h \mapsto \psi_h$, что

$$\psi_{hg} = \psi_h \cdot h(\psi_g) \quad \forall\, g, h \in G\,. \tag{5-11}$$

Эти соотношения называются *мультипликативными уравнениями Э. Нётер*. Главному дифференцированию $\delta_\zeta\colon G \to \mathbb{F}^\times$ отвечает набор $\psi_h = h(\zeta)/\zeta$. Покажем, что каждое решение

$$\psi = \{\psi_g \in \mathbb{F}^\times \mid g \in G\}$$

уравнений (5-11) имеет вид $\psi_g = g(\zeta)/\zeta$ для некоторого $\zeta \in \mathbb{F}^\times$, т. е. что мультипликативная группа когомологий $H^1(G, \mathbb{F}^\times) = 1$ тоже тривиальна. Так как мультипликативные характеры $g\colon \mathbb{F}^\times \to \mathbb{F}^\times$, где $g \in G$, линейно независимы над $\mathbb{F}$ по упр. 4.9 на стр. 40, линейный оператор $\sum_{g\in G} \psi_g \cdot g\colon \mathbb{F} \to \mathbb{F}$ ненулевой. Пусть $\zeta = \sum_{g\in G} \psi_g \cdot g(\vartheta) \in \mathbb{F}^\times$ — произвольный ненулевой элемент в его образе. Тогда для всех $h \in G$

$$h(\zeta) = \sum_{g\in G} h(\psi_g) \cdot hg(\vartheta) = \sum_{g\in G} \frac{\psi_{hg}}{\psi_h} \cdot hg(\vartheta) = \frac{\zeta}{\psi_h}\,,$$

откуда $\psi_h = h(\zeta)/\zeta$, как и утверждалось.

Теорема 5.1 (теорема 90 Гильберта)
В любом конечном циклическом расширении Галуа $\mathbb{F} \supset \Bbbk$ каждый элемент $\vartheta \in \mathbb{F}$ нормы[3] 1 имеет вид $\vartheta = g(\zeta)/\zeta$, где $\zeta \in \mathbb{F}^\times$, а g — образующая группы Галуа $G = \operatorname{Gal} \mathbb{F}/\Bbbk$.

[1] В честь Эммы Нётер.

[3] Напомню, что *нормой* $N(\vartheta)$ элемента $\vartheta \in \mathbb{F}$ называется определитель оператора умножения на ϑ: $\mathbb{F} \to \mathbb{F}$, $x \mapsto \vartheta x$, см. прим. 1.3 на стр. 6.

Доказательство. Согласно упр. 4.5 на стр. 39 норма любого элемента $\vartheta \in \mathbb{F}$ равна

$$N(\vartheta) = \prod_{g \in G} g(\vartheta)$$

и представляет собой мультипликативную запись результата применения *норменного оператора* $N = \sum_{g \in G} g \in \mathbb{Z}G$ из групповой алгебры группы G к элементу ϑ. Элементы нормы 1 образуют ядро этого оператора. В прим. 5.1 на стр. 51 мы видели, что для циклической группы G с образующей g подгруппа $\ker N \subset \mathbb{F}^\times$ изоморфна группе дифференцирований $\mathrm{Der}(G, \mathbb{F}^\times)$, и главным дифференцированиям отвечают при этом изоморфизме элементы подгруппы $\mathrm{im}(g - e) \subset \ker N$. В мультипликативной записи они имеют вид $g(\zeta)/(z)$. В предыдущем прим. 5.3 мы видели, что все дифференцирования $G \to \mathbb{F}^\times$ являются главными, что и доказывает теорему. □

Замечание 5.1. Утверждение теор. 5.1 впервые увидело свет как Теорема 90 (Satz 90) в монографии D. Hilbert, Theorie der Algebraischen Zahlkorper (1897). Для круговых расширений $\mathbb{K}_n \supset \mathbb{Q}$ этот факт впервые обнаружил Куммер, а общая формулировка из прим. 5.3 была предложена Эмми Нётер под воздействием книги Гильберта. По этой причине результаты прим. 5.3 и прим. 5.2 на стр. 52 и разные другие вариации на тему обращения в нуль первых когомологий группы Галуа в наши дни скопом именуются «теоремой 90 Гильберта».

Упражнение 5.7 (аддитивная версия теоремы 90). Докажите, что любом конечном циклическом расширении Галуа $\mathbb{F} \supset \Bbbk$ каждый бесследный элемент[1] $\vartheta \in \mathbb{F}$ имеет вид $\vartheta = g(\zeta) - \zeta$, где $\zeta \in \mathbb{F}$, а g — образующая группы Галуа $\mathrm{Gal}\,\mathbb{F}/\Bbbk$.

5.4. Изоморфизм Куммера. Всюду далее мы по умолчанию считаем, что поле $\Bbbk$ содержит примитивный корень степени n из единицы[2], и обозначаем через $\mathbb{L}^\times$ мультипликативную группу ненулевых элементов поля $\mathbb{L}$, а через $\boldsymbol{\mu}_n$ и $\mathbb{L}^{\times n}$ — её подгруппы, образованные корнями n-й степени из единицы и n-ми степенями ненулевых элементов поля $\mathbb{L}$ соответственно.

Теорема 5.2 (изоморфизм Куммера)
Пусть $\mathbb{F} \supset \Bbbk$ — конечное расширение Галуа с группой Галуа $G = \mathrm{Gal}\,\mathbb{F}/\Bbbk$. Отображение

$$\varkappa : \frac{\mathbb{F}^{\times n} \cap \Bbbk}{\Bbbk^{\times n}} \to \mathrm{Hom}(G, \boldsymbol{\mu}_n), \tag{5-12}$$

сопоставляющее классу элемента $a = \alpha^n$, где $a \in \Bbbk$, $\alpha \in \mathbb{F}$, гомоморфизм

$$\varkappa_\alpha : G \to \boldsymbol{\mu}_n, \ g \mapsto \frac{g(\alpha)}{\alpha},$$

является корректно определённым изоморфизмом мультипликативных абелевых групп.

Доказательство. Точная тройка мультипликативных G-модулей

$$1 \to \boldsymbol{\mu}_n \to \mathbb{F}^\times \xrightarrow{\vartheta \mapsto \vartheta^n} \mathbb{F}^{\times n} \to 1$$

[1] Т. е. $\mathrm{Sp}(\vartheta) = 0$, где $\mathrm{Sp}(\vartheta)$ — это след умножения на ϑ: $\mathbb{F} \to \mathbb{F}$, $x \mapsto \vartheta x$, см. прим. 1.3 на стр. 6.
[2] См. n° 4.2 на стр. 39.

порождает длинную точную последовательность когомологий из форм. (5-7) на стр. 50, начало которой имеет вид

$$1 \to \boldsymbol{\mu}_n \to \Bbbk^\times \xrightarrow{t\mapsto t^n} \mathbb{F}^{\times n} \cap \Bbbk \xrightarrow{\delta} H^1(G, \boldsymbol{\mu}_n) \to 1\,,$$

где самая правая группа $H^1(G, E^\times) = 1$ по мультипликативной теореме Э. Нётер из прим. 5.3 на стр. 52, а гомоморфизм δ переводит класс элемента $a = \alpha^n$ по модулю $\Bbbk^{\times n}$ в класс дифференцирования $g \mapsto g(\alpha)/\alpha$ по модулю $\mathrm{PrDer}(G, \boldsymbol{\mu}_n)$. Тем самым отображение из условия теоремы корректно задаёт изоморфизм $(\mathbb{F}^{\times n} \cap \Bbbk)/\Bbbk^{\times n} \xrightarrow{\sim} H^1(G, \boldsymbol{\mu}_n)$. Так как $\boldsymbol{\mu}_n \subset \Bbbk$, группа G действует на $\boldsymbol{\mu}_n$ тривиально. Поэтому мультипликативная версия правила Лейбница из форм. (5-6) на стр. 49 редуцируется до условия $\psi(gh) = \psi(g)\psi(h)$, означающего, что $\mathrm{Der}(G, \boldsymbol{\mu}_n) = \mathrm{Hom}(G, \boldsymbol{\mu}_n)$, а отвечающие элементам $\xi \in \boldsymbol{\mu}_n$ главные дифференцирования $\delta_\xi : g \mapsto g(\xi)/\xi = 1$ тривиальны. Мы заключаем, что $H^1(G, \boldsymbol{\mu}_n) = \mathrm{Hom}(G, \boldsymbol{\mu}_n)$. □

Следствие 5.6
Если показатель[1] группы Галуа G конечного абелева расширения Галуа $\mathbb{F} \supset \Bbbk$ делит n, то (мультипликативные) абелевы группы $(\mathbb{F}^{\times n} \cap \Bbbk)/\Bbbk^{\times n}$ и G двойственны друг другу по Понтрягину[2]. Билинейное над $\mathbb{Z}$ совершенное спаривание $G \times (\mathbb{F}^{\times n} \cap \Bbbk)/\Bbbk^{\times n} \to \boldsymbol{\mu}_n$ между ними задаётся формулой $(g, \alpha) \mapsto g(\alpha)/\alpha$. □

5.5. Куммеровы расширения. Фиксируем алгебраическое замыкание $\overline{\Bbbk}$ поля $\Bbbk$, содержащего примитивный корень степени n из единицы. Будем называть *куммеровым полем* показателя n всякое содержащееся в $\overline{\Bbbk}$ конечное расширение Галуа поля $\Bbbk$ с абелевой группой Галуа G, показатель которой делит[3] n. В этом разделе мы классифицируем все такие расширения.

Предложение 5.2
Каждое куммерово поле является полем разложения над $\Bbbk$ многочлена вида

$$\prod_i (x^{m_i} - a_i)\,,\ \text{где } a_i \in \Bbbk \text{ и } m_i \mid n \text{ при всех } i\,, \tag{5-13}$$

и наоборот, все такие поля разложения являются куммеровыми.

Доказательство. Так как $\Bbbk$ содержит первообразный корень n-й степени из единицы, $\mathrm{char}\,\Bbbk \nmid n$, а каждый многочлен вида $x^m - a$, где $a \in \Bbbk$ и $m \mid n$, сепарабелен и по теор. 4.1 на стр. 39 имеет над $\Bbbk$ циклическую группу Галуа, порядок которой делит n. Поэтому поле разложения любого многочлена (5-13) является куммеровым. Наоборот, каждая абелева группа G, показатель которой делит n, имеет композиционный ряд, факторами которого являются простые циклические группы, порядки которых делят[4] n. Согласно соответствию Галуа, каждое куммерово поле $\mathbb{F} \supset \Bbbk$ с группой Галуа G является верхним этажом башни циклических расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_m = \mathbb{F}\,,\ \text{где } \mathbb{L}_{i+1} = \mathbb{L}_i[\vartheta_i^{1/q_i}] \simeq \mathbb{L}_i[x]/(x^{q_i} - \vartheta_i)\,. \tag{5-14}$$

[1] Напомню, что *показателем* группы G называется наименьшее такое $n \in \mathbb{N}$, что $g^n = e$ для всех $g \in G$.

[2] Т. е. каждая из них является группой мультипликативных характеров другой группы со значениями в $\boldsymbol{\mu}_n \subset \Bbbk \subset \overline{\Bbbk}$, см. теорему 2.3 на с. 22 лекции 2 моего курса Алгебра-2.

[3] Таким образом, порядки всех элементов группы Галуа куммерова поля делят n. В частности, порядок самой группы Галуа не делится на $\mathrm{char}\,\Bbbk$.

[4] Так $\mathrm{char}\,\Bbbk \nmid n$, порядки всех факторов отличны от $\mathrm{char}\,\Bbbk$, и тем самым $\mathrm{char}\,\Bbbk \nmid |G|$.

По теор. 4.2 на стр. 40 и теор. 4.1 на стр. 39 каждый этаж $\mathbb{L}_{i+1}$ является полем разложения неприводимого над $\mathbb{L}_i$ двучлена $f_i(x) = x^{q_i} - \vartheta_i$ с простым $q_i \mid n$ и $\vartheta_i \in \mathbb{L}_i^\times \smallsetminus \mathbb{L}_i^{\times q_i}$, и получается присоединением к $\mathbb{L}_i$ какого-нибудь одного из отличающихся друг от друга множителем из $\boldsymbol{\mu}_{q_i} \subset \Bbbk$ корней $\vartheta_i^{1/q_i} \in \overline{\Bbbk}$ двучлена f_i. Поскольку произведение $\prod_{\xi \in \boldsymbol{\mu}_{q_{i-1}}} (x^{q_i} - \xi\vartheta_i) = x^{q_i q_{i-1}} - \vartheta_i^{q_{i-1}}$ инвариантно относительно группы Галуа $\operatorname{Gal}\mathbb{L}_i/\mathbb{L}_{i-1} \simeq \boldsymbol{\mu}_{q_{i-1}}$, число $\vartheta_i^{q_{i-1}} \in \mathbb{L}_{i-1}$. Продолжая этот спуск до самого нижнего этажа башни, заключаем, что $\vartheta_i^{q_{i-1}\cdots q_0} \in \Bbbk$. Таким образом, ϑ_i^{1/q_i} является корнем многочлена $x^{n_i} - b_i$, где $n_i = q_0 q_1 \ldots q_i \mid n$ и $b_i = \vartheta_i^{q_{i-1}\cdots q_0} \in \Bbbk$. По теор. 4.1 на стр. 39 минимальный многочлен элемента ϑ_i^{1/q_i} над $\Bbbk$, будучи неприводимым делителем многочлена $x^{n_i} - b_i$, тоже имеет вид $x^{m_i} - a_i$, где $a_i \in \Bbbk$ и $m_i \mid n_i \mid n$. Так как поле $\mathbb{F}$ нормально над $\Bbbk$, оно содержит поле разложения многочлена $x^{m_i} - a_i$. Будучи порождённым корнями ϑ_i^{1/q_i} этих многочленов, $\mathbb{F}$ является полем разложения их произведения $\prod_i (x^{m_i} - a_i)$. □

Предложение 5.3
Степень $[\mathbb{F} : \Bbbk]$ любого куммерова поля $\mathbb{F} \supset \Bbbk$ показателя n равна индексу подгруппы $\Bbbk^{\times n}$ в мультипликативной группе $\mathbb{F}^{\times n} \cap \Bbbk$.

Доказательство. Степень $[\mathbb{F} : \Bbbk]$ равна порядку группы Галуа $G = \operatorname{Gal}\mathbb{F}/\Bbbk$. Согласно теор. 5.2 двойственная по Понтрягину группа $G^\wedge = \operatorname{Hom}(G, \overline{\Bbbk}) = \operatorname{Hom}(G, \boldsymbol{\mu}_n)$ изоморфна факторгруппе $(\Bbbk \cap \mathbb{F}^{\times n})/\Bbbk^{\times n}$. Так как $\operatorname{char}\Bbbk \nmid |G|$, множество $G^\wedge$ мультипликативных характеров группы G составляет базис в пространстве $\overline{\Bbbk}^G$ всех функций[1] $G \to \overline{\Bbbk}$. Поэтому $|G| = |G^\wedge|$. □

Теорема 5.3
Отображение $p : \mathbb{F} \mapsto \mathbb{F}^{\times n} \cap \Bbbk$, сопоставляющее полю $\mathbb{F} \supset \Bbbk$ мультипликативную группу ненулевых элементов поля $\Bbbk$, из которых в поле $\mathbb{F}$ извлекается корень n-й степени, и отображение $r : B \mapsto \Bbbk[B^{1/n}] \subset \overline{\Bbbk}$, сопоставляющее мультипликативной подгруппе $B \subset \Bbbk^\times$ наименьшее расширение поля $\Bbbk$, содержащее все корни n-й степени из всех элементов группы B, являются взаимно обратными биекциями между куммеровыми полями $\Bbbk \subset \mathbb{F} \subset \overline{\Bbbk}$ показателя n и мультипликативными подгруппами $\Bbbk^{\times n} \subset B \subset \Bbbk^\times$ с конечным индексом $[B : \Bbbk^{\times n}]$. При этом $[\mathbb{F} : \Bbbk] = [B : \Bbbk^{\times n}]$ для всех соответствующих друг другу $\mathbb{F}$ и B.

Доказательство. Для каждого куммерова поля $\mathbb{F}$ группа $p(\mathbb{F})$ имеет согласно предл. 5.3 конечный индекс $[p(\mathbb{F}) : \Bbbk^{\times n}] = [\mathbb{F} : \Bbbk]$. Наоборот, если $\Bbbk^{\times n} \subset B \subset \Bbbk^\times$ и $[B : \Bbbk^{\times n}] < \infty$, поле $\Bbbk[B^{1/n}]$ является полем разложения многочлена $\prod_a (x^n - a)$, где a пробегает конечный набор представителей смежных классов $B/\Bbbk^{\times n}$, и тем самым куммерово. Поэтому оба отображения $p : \mathbb{F} \mapsto \mathbb{F}^{\times n} \cap \Bbbk$ и $r : B \mapsto \Bbbk[B^{1/n}] \subset \overline{\Bbbk}$ корректно определены. Очевидно, что $rp(\mathbb{F}) \subset \mathbb{F}$ для любого поля $\mathbb{F} \supset \Bbbk$ и $B \subset pr(B)$ для любой группы $B \supset \Bbbk^{\times n}$. Остаётся убедиться, что оба включения являются равенствами, если степень $[\mathbb{F} : \Bbbk]$ и индекс $[B : \Bbbk^{\times n}]$ конечны.

Рассмотрим сначала включение $rp(\mathbb{F}) \subset \mathbb{F}$. По предл. 5.3 для любого куммерова поля $\mathbb{L}$

$$[\mathbb{L} : \Bbbk] = [p(\mathbb{L}) : \Bbbk^{\times n}]. \tag{5-15}$$

[1] Поскольку $\operatorname{char}\Bbbk \nmid |G|$, представление конечной абелевой группы G в пространстве функций $\overline{\Bbbk}^G$ является прямой суммой одномерных неприводимых представлений. Легко видеть, что изотипный G-подмодуль в $\overline{\Bbbk}^G$, на котором G действует умножением на характер $\chi \in G^\wedge$, одномерен и состоит из всех функций, пропорциональных обратному характеру $\chi^{-1} : G \to \overline{\Bbbk}$, $g \mapsto \chi(g)^{-1} = \chi(g^{-1})$, см. раздел 2.4.2 на с. 21 лекции 2 моего курса Алгебра-2.

Тогда

$$\begin{aligned} [\mathbb{F} : \Bbbk] &\geqslant [rp(\mathbb{F}) : \Bbbk] && \text{(так как } rp(\mathbb{F}) \subset \mathbb{F}) \\ [rp(\mathbb{F}) : \Bbbk] &= [prp(\mathbb{F}) : \Bbbk^{\times n}] && \text{(это (5-15) для } \mathbb{L} = rp(\mathbb{F})) \\ [prp(\mathbb{F}) : \Bbbk^{\times n}] &\geqslant [p(\mathbb{F}) : \Bbbk^{\times n}] && \text{(так как } p(\mathbb{F}) \subset prp(\mathbb{F}))\,. \end{aligned}$$

Но $[\mathbb{F} : \Bbbk] = [p(\mathbb{F}) : \Bbbk^{\times n}]$ по той же формуле (5-15). Поэтому оба написанных выше неравенства являются равенствами. В частности, $[\mathbb{F} : \Bbbk] = [rp(\mathbb{F}) : \Bbbk]$, и тем самым $\mathbb{F} = rp(\mathbb{F})$.

Теперь рассмотрим включение $B \subset pr(B)$. Обозначим группу Галуа поля $r(B) = \Bbbk[B^{1/n}]$ через $G = \operatorname{Gal} r(B)/\Bbbk$. Изоморфизм Куммера из теор. 5.2 на стр. 53

$$\varkappa : \frac{r(B)^{\times n} \cap \Bbbk}{\Bbbk^{\times n}} \xrightarrow{\sim} G^\wedge = \operatorname{Hom}(G, \boldsymbol{\mu}_n)$$

переводит класс элемента $b = \beta^n$, $b \in B$, $\beta \in \Bbbk[B^{1/n}]$, в гомоморфизм

$$\varkappa_b : G \to \boldsymbol{\mu}_n\,,\ g \mapsto \frac{g(\beta)}{\beta}\,,$$

и изоморфно отображает подгруппу $B/\Bbbk^{\times n} \subset pr(B)/\Bbbk^{\times n}$ на некоторую подгруппу $\varkappa(B) \subset G^\wedge$.

Упражнение 5.8 (двойственность Понтрягина). Убедитесь, что между подгруппами двойственных по Понтрягину конечных абелевых групп G и $G^\wedge = \operatorname{Hom}(G, \boldsymbol{\mu}_n)$ показателя $m \mid n$ имеется каноническая оборачивающая включения инволютивная биекция, сопоставляющая каждой подгруппе $K \subset G^\wedge$ подгруппу $K^* = \bigcap_{\chi \in K} \ker \chi \subset G$.

Двойственная к $\varkappa(B) \subset G^\wedge$ подгруппа $H = \bigcap_{b \in B} \ker \varkappa_b \subset G$ состоит из всех таких $g \in G$, что $g(\beta) = \beta$ для любого $\beta \in \overline{\Bbbk}$ с $\beta^n \in B$. Поскольку такие β порождают поле $r(B)$ над $\Bbbk$, подгруппа $H \subset \operatorname{Gal} r(B)/\Bbbk$ состоит только из тождественного преобразования. Тем самым, двойственная к ней подгруппа $\varkappa(B) \subset G^\wedge$ совпадает с $G^\wedge$, а значит $B = pr(B)$. □

Ответы и указания к некоторым упражнениям

Упр. 5.1. Для любого базиса $f_1, \dots, f_n$ поля $\mathbb{F}$ как векторного пространства над $\Bbbk$ подпространства $f_i \otimes_{\Bbbk} \mathbb{F} \subset W$ изоморфны $\mathbb{F}$ и пространство W является их прямой суммой.

Упр. 5.2. Так как $\psi(e) = \psi(e \cdot e) = \psi(e) \cdot e + e \cdot \psi(e) = \psi(e) + \psi(e)$, вычитая из обеих частей $\psi(e)$, получаем $\psi(e) = 0$.

Упр. 5.3. Если $\psi_1(gh) = \psi_1(g) + g\psi_1(h)$ и $\psi_2(gh) = \psi_2(g) + g\psi_2(h)$, то

$$\psi_1 + \psi_2 \colon gh \mapsto \psi_1(g) + g\psi_1(h) + \psi_2(g) + g\psi_2(h) = \psi_1(g) + \psi_2(g) + g(\psi_1(h) + \psi_2(h)),$$

что и утверждается.

Упр. 5.6. Так как $N(e-g) = (e-g)N = 0$ и $Nz = \varepsilon(z) \cdot N$ для всех $z \in \mathbb{Z}C_n$, мы заключаем, что $\operatorname{im} N \subset \ker(g-e)$ и $\operatorname{im}(g-e) \subset \ker N = \ker \varepsilon$. Каждый элемент $z = \sum_{\nu=0}^{n-1} z_\nu g^\nu \in \mathbb{Z}C_n$ записывается в виде $z = \varepsilon(z) \cdot N + \sum_{\nu=1}^{n-1} z_\nu (g^\nu - e)$. Если $\varepsilon(z) = 0$, то z лежит в линейной оболочке векторов $g^\nu - e = (g-e)(e + g + \dots + g^{\nu-1}) \in \operatorname{im}(g-e)$. Если $(g-e)z = 0$, то $z_0 = z_1 = \dots = z_{n-1}$ и $z = z_0 N = z_0 N e \in \operatorname{im} N$.

Упр. 5.8. Отождествим G с $G^{\wedge\wedge}$ при помощи канонического изоморфизма $G \xrightarrow{\sim} G^{\wedge\wedge}$, $g \mapsto \mathrm{ev}_g$, где

$$\mathrm{ev}_g \colon G^\wedge \to \Bbbk, \ \chi \mapsto \chi(g).$$

Тогда двойственной к $H \subset G = G^{\wedge\wedge}$ подгруппой в $G^\wedge$ будет подгруппа

$$H^* = \{\chi \colon G \to \boldsymbol{\mu}_n \mid H \subset \ker \chi\} = \operatorname{Hom}(G/H, \boldsymbol{\mu}_n) \subset \operatorname{Hom}(G, \boldsymbol{\mu}_n)$$

(вложение $\operatorname{Hom}(G/H, \boldsymbol{\mu}_n) \hookrightarrow \operatorname{Hom}(G, \boldsymbol{\mu}_n)$ переводит характер $G/H \to \boldsymbol{\mu}_n$ в его композицию с гомоморфизмом факторизации $G \twoheadrightarrow G/H$), откуда $|H^*| = |(G/H)^\wedge| = |G/H| = |G|/|H|$, и стало быть $|H^{**}| = |H|$. Поэтому очевидное включение $H \subset H^{**}$ является равенством.