4. Разложения идеалов в расширениях

AKBL:

A - дедекиндово кольцо

$K = Q(A)$ - поле частных

L - кон. сепарабельное расширение поля K, $[L:K] = n$

$B = \overline{A}^L$ - целое замыкание A в L

(известно B - тоже дедекиндово)

Общая задача: $\forall\ 0 \neq I \lhd A$ $I = P_1^{r_1} \cdot \ldots \cdot P_n^{r_n}$

P_i - простые идеалы, найти разложение $IB \trianglelefteq B$

на простые идеалы в B (IB - собств. дов-ва на семинаре)

Доп. работа в семестре 5.

Естественно посмотреть на разложение pB в B,

где p - простой идеал в A.

Опр. Пусть $AKLB$, $p \trianglelefteq A$ простой и $pB = P_1^{e_1} \dots P_g^{e_g}$ — разложение в B идеала pB на простые идеалы $P_1, \dots P_g$. Число $e_i = e(P_i/p) > 0$ наз-ся индексом ветвления идеала P_i над p. Если $P \trianglelefteq B$ простой не входит в разложение pB, то полагают $e(P/p) = 0$. Говорят, что идеал p разветвляется в кольце B (или L), если $\exists i \in \{1, \dots g\} : e(P_i/p) > 1$. Если pB — простой идеал в B, то говорят, что p инертен в L.

Лемма 1 Пусть $AKLB$, $p \trianglelefteq A$, $P \trianglelefteq B$ ненулевые простые идеалы. Тогда $e(P/p) > 0 \Leftrightarrow P \cap A = p$.

Д-во: $\Leftarrow$ $p = P \cap A \subseteq P \Rightarrow pB \subseteq P \Rightarrow P$ входит в разл. идеала pB (см. ОТА) $\Rightarrow e(P/p) > 0$.

(⇐) $pB = p^e(\ ) \Rightarrow p \subseteq pB \subseteq P \Rightarrow p \subseteq P \cap A$.

Но $P \cap A \neq A$, т.к. $1 \notin P$. Т.к. p – идеал и A – кольцо.

$\Rightarrow p \overset{\text{нек}}{\lhd} A \Rightarrow p = P \cap A$ ▣

Если P входит в разложение pB, то $p = P \cap A \Rightarrow$

Вл-е $A \to B$ индуцирует вл-е поля A/p в поле B/p по правилу $a + p \mapsto a + P$. Т.к. B – к.п. над A-модулем (Ст. 1.4.1 о целом базисе из АКТЗ), то $\dim_{A/p} B/p < \infty$

Опр 2 Пусть $A \subset L \subset B$ и P входит в разложение pB в B.

Число $f(P/p) = [B/p : A/p] = \dim_{A/p} B/p$ наз-ся

Индексом инерции идеала P над p.

(или относительной степенью)

Т. 1 (фундаментальное тождество)

Пусть $A \subset L \supset B$, $p \lhd A$ - некум. простой, $pB = P_1^{e_1} \cdot \ldots \cdot P_g^{e_g}$, где $P_i \lhd B$ - некум. простые и $e_i = e(P_i/p) \geq 0$, $f_i = f(P_i/p)$, для $i = 1, \ldots, g$. Тогда

$$(*) \quad \sum_{i=1}^{g} e_i f_i = n = [L : K].$$

Если дополнительно, L/K - расширение Галуа, то

$\forall i = 1 \ldots g$, $e_i = e$, $f_i = f$, т.е. $\boxed{efg = n}$.

Д-во: Сначала общий случай:

Обозн: $F = A/p$ (это поле).

1) Д-ем, что $\dim_F B/pB = n$.

Зам: B/pB – в.п над F, гл. операция умн-я на скаляр:

$(a+p)(b+pB) = ab+pB$, $a \in A$, $b \in B$, определена корректно.

Сначала рассм-м случай, когда A – обл. гл. идеалов, т.е.

$B = Ax_1 + \dots + Ax_n$ – свободный A-модуль ранга n

(по т-ме 3.4.1 о целом базисе из ANT3).

$\forall b \in B \; b = a_1x_1 + \dots + a_nx_n$, $a_i \in A \Rightarrow$

$b+pB = (a_1+p)(x_1+pB) + \dots + (a_n+p)(x_n+pB) \Rightarrow$

$\langle x_1+pB, \dots, x_n+pB \rangle = B/pB$. Осталось д-ть, что

$x_1+pB, \dots x_n+pB$ – лин. независимы. Пусть $v \in pB$, т.е.

$v+pB = 0+pB$. Тогда $v = \sum\limits_{i=1}^{n} a_i x_i = \sum c_k y_k$, $c_k \in p$, $y_k \in B$.

Разложим y_k по $x_1, \dots, x_n$: $y_k = \sum\limits_{i=1}^{n} a_{ki} x_i$ в B.

Тогда $v = \sum_k c_k u_k = \left(\sum_k c_k a_{k1}\right) x_1 + \ldots + \left(\sum_k c_k a_{kn}\right) x_n$.

В силу м.н.о. $x_1 \ldots x_n$ – базис свободного A-модуля B,

$\forall i = 1 \ldots n$ имеем $a_i = \sum_k c_k a_{ki} \in \mathfrak{p} \Rightarrow q_i + \mathfrak{p} = 0$, ч.т.д.

Если A – нетерово дедекиндово кольцо, то $\mathfrak{p}$-м его можно задать $A_{\mathfrak{p}} = A_S$, где $S = A \setminus \mathfrak{p}$. На семинаре д-м, что $\overline{A_{\mathfrak{p}}}^{L} = B_{\mathfrak{p}}$. Кольцо $A_{\mathfrak{p}}$ – обл. гл. идеалов.

Кроме того, $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \simeq A/\mathfrak{p} = F$ по утв. 2.1.4

$\dim_F B/\mathfrak{p} = \dim_{A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}} B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} = n$ по доказанному выше,

если мы д-м, что $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \simeq B/\mathfrak{p}B$. По утв.

Идеалы $P_1 \dots P_s$ в B, не пересекаются с S, т.к $P_i \subsetneq pB$ в виду того, что P_i входит в разложение pB. Поэтому р-во

$$pB = P_1^{\alpha_1} \dots P_s^{\alpha_s} \Rightarrow pB_p = (P_1 B_p)^{\alpha_1} \dots (P_s B_p)^{\alpha_s} \overset{\text{кто}}{\Rightarrow}$$

$$B_p / pB_p \simeq \bigoplus_{i=1}^{s} B_p / (P_i B_p)^{e_i} \overset{\text{пред. 2.4.1}}{\simeq} \bigoplus_{i=1}^{g} B / P_i^{e_i} \overset{\text{кто}}{\simeq} B / pB.$$

Тем самым р-во $\dim_F B/pB = n$ окончательно доказано.

2) A - ев, что $\dim_F B / P_i^{e_i} = e_i f_i$.

Замечание: $V = B / P_i^{e_i}$ - в.п над $A/p = F$, т.к. корректно:

$(a+p)(b+P_i^{e_i}) = ab + P_i^{e_i}$, $a \leftrightarrow b \subset B$ в силу $pB \subseteq P_i^{e_i}$

$$V = B/p \supset P_i/p \supset P_i^2/p \supset \dots \supset P_i^{e_i-1}/p \supset P_i^{e_i}/p = 0$$

$$V_0 \quad V_1 \quad V_2 \quad \dots \quad V_{e_i-1} \quad V_{e_i}$$

$$\dim_F V = \sum_{i=1}^{e_i} \dim V_{i-1}/V_i .$$

Имеем $V_0/V_1 = B/P^{e_i}/P_i/P^{e_i} \simeq B/P_i \Rightarrow \dim V_0/V_1 = f(P_i/p)$

$= f_i$ по опр. индекса инерции.

Заметим, что $\Phi = B/P_i$ — поле и $[\Phi : F] = f_i$.

$V_{k-1}/V_k = P_i^{k-1}/P_i^{e_i}/P_i^k/P_i^{e_i} \simeq P_i^{k-1}/P_i^k$ при $k = 2, \dots, e_i$.

P_i^{k-1}/P_i^k — в.п. над Φ, т.к. $(\forall t \in P_i)(v + P_i^k) = tv + P_i^k$

($v \in P_i^{k-1}$, $tv \in P_i^{k-1}$)

$\Rightarrow \dim_F (V_{k-1}/V_k) = \dim_\Phi (V_{k-1}/V_k) \cdot |\Phi : F|$.

$\dim_F \left(V_{k-1} / V_k \right) = 1$, т.к. V_{k-1} / V_k не содержит

ф-ий. нетр. собств. подпр-в, иначе $\exists I \trianglelefteq B$:

$P_i^k \subsetneq I \subsetneq P_i^{k-1} \Rightarrow 0 \neq I / P_i^k \trianglelefteq B / P_i^k$, что

противоречит следствию Т. 2.1.2 из ANT 4.

Поэтому $\dim_F \left(V_k / V_{k-1} \right) = f_i \quad \forall k = 1, \dots n \Rightarrow$

$\dim_F V = \sum_{k=1}^{e_i} \dim_F \left(V_k / V_{k-1} \right) = e_i f_i$, ч.т.д.

3) В силу КТО: $\rho B = P_1^{e_1} \dots P_g^{e_g} \Rightarrow$

$B / \rho B \simeq \bigoplus_{i=1}^{g} B / P_i^{e_i} \Rightarrow n = \dim B / \rho B = \sum_{i=1}^{g} \dim B / P_i^{e_i} = \sum_{i=1}^{g} e_i f_i$

(1) (2)

Т-ма доказана в общем случае.

Пусть теперь L/K – расширение Галуа, т.е. $|G| = |L:K| = n$, где $G = \{\sigma \in Aut_K(L)\}$ – группа Галуа расш. L/K.

Упр1 $\forall \sigma \in G$: σ_B – из-м B, тождеств. на A.

Указ: $x \in B \Rightarrow \sigma(x) \in B$, т.к. ур-я целой зав-ти сохр-ся.

Вчастности, $0 \neq P \trianglelefteq B$ – прост. $\Rightarrow \sigma(P) \trianglelefteq B$ – прост. и т.ч. $P \cap A \Rightarrow \sigma(P) = P$.

Достаточно док-ть, что G действует транзитивно на мн-ве $P_1, \dots P_g$ простых идеалов в разложении $pB = P_1^{e_1} \dots P_g^{e_g}$. Дей-но, если $\forall i,j \in \{1..g\}$ $\exists \sigma: \sigma(P_i) = P_j$, то $pB = \sigma(pB) = \sigma(P_1)^{e_1} \dots \sigma(P_i)^{e_i} \dots \sigma(P_g)^{e_g} \Rightarrow e_i = e_j$ в силу единств. разложения pB. Кроме того, $\sigma(P_i) = P_j \Rightarrow B/P_i \cong B/P_j$ с индук. $A/p \Rightarrow f_i = f_j$

Замечание, что G действует на $\{P_1, \dots P_g\}$, т.к. $Q \in \{P_1, \dots P_g\}$
$\Leftrightarrow p \subseteq Q$, а $\sigma(p) = p$. Предп., что это действие
не транзитивно и P_1 и P_2 лежат в разн. орбитах.
По КТО (т. 2.2.1 из ANT5) $\exists x \in P_1 : x \notin Q \; \forall Q \in P_2^G$
– орбита P_2 отн-но действия группы G. Тогда $a = N_{L/K}(x)$
В силу условия $A \; a \in A$. Применяем ф-ту из
предл. 1.3.3 $a = \prod_{\sigma \in G} \sigma^{-1}(x)$. т.к. $id \in G \Rightarrow a \in P_1$.
По лемме 1 $a \in p = P_1 \cap A$. Но $p = P_2 \cap A$ по той же
лемме $\Rightarrow a \in P_2$. Т.к. идеал P_2 – простой в B
хотя бы один из эл-тов $\sigma^{-1}(x)$, $\sigma \in G$, должен
лежать в P_2, но тогда $x \in Q$ для $Q \in P_2^G$, противоречие

Заметим, что любое кольцевое расш. L поля K сепарабельно (т.к. $\mathrm{char} K = 0$), поэтому если L - поле разложения мин-на f, то для $\mathcal{O}_L$ верна сильная версия т. 1.

Т. 2 (Дедекинд–Куммер) Пусть $AKLB$, A - дед., $|L:K| = n$, $0 \neq p \overset{\text{прост.}}{\lhd} A$, $F = A/p$ - поле. Допустим $B = A[\alpha]$, т.е. $\exists \alpha \in B$: $1, \alpha, \dots \alpha^{n-1}$ - целый базис в B, а минимальные $g_i(t) \in A[t]$ таковы, что $\mu^{\alpha}_{K}(t) = \overline{g_1^{e_1}}(t_\alpha) \dots \overline{g_m^{e_m}}(t_m)$ разложение мин. мн-на α неприводимые в $F[t]$. Тогда

$$pB = P_1^{e_1} \dots P_m^{e_m}, \text{ где } P_i = (p, g_i(\alpha)), f(P_i/p) = \deg g_i,$$

– разложение на простые идеалы в B.

Δ-во: 1) $P_i = (p, g_i(\alpha)) \lhd B$ – простой и $f_i = f(P_i/p) = \deg g_i$.

Оп-е $\varphi : A[t] \to B$, т.ч. $\varphi(t) = \alpha$, – гом-зм на B.

и $\ker \varphi = (\mu^{\alpha}_{L/K}(t))$ – идеал, порожд. $\mu^{\alpha}_{L/a}(t)$.

По т-ме $B/(p, g_i(\alpha)) \simeq A[t]/(p, g_i(t), \mu^{\alpha}_{L/K}(t)) \simeq F[t]/(\overline{g_i(t)})$

$\because g(t) - g(\alpha) \in (\mu^{\alpha}(t))$, $\because g_i$ делит $\mu^{\alpha}_{L/K}$

Т.к. $\overline{g_i(t)} \in F[t]$ неприводим $\Rightarrow F[t]/(\overline{g_i(t)})$ – поле $\Rightarrow$

P_i – простой идеал. Кроме того, из этого же изоморфизма $\Rightarrow$

$f_i = \dim_F (B/P_i) = \deg g_i$.

2) $P_1^{e_1} \dots P_m^{e_m} \subseteq pB$, где $P_i = (p, g_i(\alpha))$

$x \in P_i \Rightarrow x = p + g_i(\alpha) b$, $b \in B$, $p \in pB \Rightarrow$

$y \in P_i^{e_i} \Rightarrow y = p + g_i(\alpha)^{e_i} b$, $b \in B$, $p \in pB \Rightarrow$

$z \in P_1^{e_1} \dots P_m^{e_m} \Rightarrow z = p + \mu^{\alpha}_{L/k}(\alpha) \cdot b \in pB$ ч.т.д.

$= 0$

3) $P_i \neq P_j$ при $i \neq j$. Исп. $B = A[\alpha]$, т.к $1, \alpha \dots \alpha^{n-1}$ - целый базис $\Rightarrow pB = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in p\}$.

Если $P_i \subseteq P_j = (p, g_j(\alpha)) = pB + g_j(\alpha)B \subseteq B = A[\alpha]$, то

$g_i(\alpha) \in P_j$, т.е. $\exists b \in B$: $g_i(\alpha) - g_j(\alpha) b \in pB$, где

$b = a_0 + \dots + a_{n-1}\alpha^{n-1} = h(\alpha)$, $a_i \in A$. $\Rightarrow g_i(\alpha) - g_j(\alpha)h(\alpha) \in pB \Rightarrow$

$f(t) = g_i(t) - g_i(t)h(t) \in (\mu^{\alpha}_{L/k}(t)) \Rightarrow (\bar{g_i}, \bar{g_j}) \neq 1$ противоречие.

4) Мы знаем, что $pB = P_1^{e_1'} \cdots P_m^{e_m'}$, где $e_i' \geq e_i$ в силу п. 1 и 2. В силу Т. 1 $\Rightarrow e_1' f_1 + \ldots + e_m' f_m = n =$

$= \deg \mu_{L/K}^{\alpha} = \sum_{i=1}^{m} e_i \cdot \deg g_i = \sum e_i f_i \Rightarrow e_i' = e_i \ \forall i$

(f_i по 1)

Замечание. Условие $B = A[\alpha]$ в ТДК (7.2) может вообще говоря не выполняться в $\mathcal{O}_L$, где L – числ. пол.

Упр 2. Пусть $L = \mathbb{Q}[\theta]$, $\theta^3 - \theta^2 - 2\theta - 8 = 0$.

Доказать, что $\frac{\theta + \theta^2}{2} \in \mathcal{O}_L$, вычислите $\mathcal{O}_L$, и покажите, что $\mathcal{O}_L$ не имеет целого базиса вида $1, \alpha, \alpha^2$.

Пусть $A \subset K \subset B$ и $pB = P_1^{e_1} \cdots P_g^{e_g}$ – разложение pB в B. Напомним, что p разветвляется в B, если $\exists i \in \overline{1..g} : e_i > 1$.

Теорема 3 (Критерий разветвл. простого идеала в расш.)

Пусть L – алг. числовое поле, p – простое число.

Идеал $P = p\mathcal{O}_L$ разветвляется в $\mathcal{O}_L \iff p \mid \operatorname{disc}(\mathcal{O}_L/\mathbb{Z})$.

В частности, $\exists$ только кон. число $p \in \mathbb{Z}$ т.ч. $p\mathcal{O}_L$ разв. в $\mathcal{O}_L$.

Д-во: Мы д-ли т. 3 только при доп. условии из ТДК: $B = \mathcal{O}_L = \mathbb{Z}[\alpha]$ для некот. $\alpha \in B$.

В условиях ТДК $\operatorname{disc}(\mathcal{O}_L/\mathbb{Z}) = D(1, \alpha, \ldots \alpha^{n-1}) = \operatorname{Dis}(\mu^{\alpha}_{L/\mathbb{Q}})$

$\operatorname{Dis}(\mu^{\alpha}_{L/\mathbb{Q}}(t)) = 0$ над полем $\mathbb{Z}/p\mathbb{Z} \iff \exists i : e_i > 1$

Упр 3 Д-те Т 3 без исп ТДК (сами разберите её д-во в записках Губарева – Предл. 2.6).

Примеры 1) $L = \mathbb{Q}[\sqrt{-5}]$, $B = O_L = \mathbb{Z}[\sqrt{-5}]$ $|L:\mathbb{Q}| = n = 2$

$p = 2\mathbb{Z} \trianglelefteq \mathbb{Z}$ $pB = (2) \trianglelefteq B$ $pB = P^2$, где

$P = (2, 1+\sqrt{5})$. Здесь $g = 1$ $e(P/p) = 2$, $f(P/p) = 1$

Идеал p разветвляется в B ($2 \mid 4m = disc(B/\mathbb{Z})$).

2) $L = \mathbb{Q}[\sqrt{5}]$, $B = O_L = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, $p = 2\mathbb{Z}$

$pB = (2)^1$ – простой идеал в B, $g = 1$, $e = 1$, $f = 2$

Идеал p не разветвляется в B ($2 \nmid m = disc(B/\mathbb{Z})$)

Упр 4 Д-ть утв-я в примерах 1 и 2. Для каких p разветвл. идеалы $p\mathbb{Z}$-в в O_L в примерах 1 и 2?