3. Поля алгебраических чисел

Все кольца предполагаются коммутативными с единицей, а гомоморфизмы колец - сохраняющими единицу.

Расширения колец.

Расширение колец B/A назывется целым, если все элементы B целы над A, и конечным, если B - конечнопорожденный модуль над A.

Конечное расширение является целым. Если B/A и C/B конечны, то и C/A конечно.

Если B/A цело, и при этом B конечно порождено, как A - алгебра, то B/A конечно.

Подмножество в B, состоящее из всех элементов, целых над A, называется целым замыканием A в B. Оно является подкольцом.

Нетеровы целозамкнутые области (NICD)

Если $\mathcal{O}$ - NICD, а $\mathfrak{p} \subset \mathcal{O}$ - простой идеал, то локальное кольцо $\mathcal{O}_{\mathfrak{p}}$ - тоже NICD.

Лемма. Пусть $\mathcal{O}$ - нётерово кольцо, M- конечнопорожденный $\mathcal{O}$ - модуль, $N \subset M$ - любой подмодуль. Тогда N конечно порожден. Если M свободен ранга n, то N также свободен, и его ранг не превосходит n.

Теорема (3.7). Пусть $\mathcal{O}$ - NICD, $k = \mathcal{O}_{(0)}$ - его поле частных, K/k - конечное сепарабельное расширение. Тогда
1) Целое замыкание $\mathcal{O}_K$ кольца $\mathcal{O}$ в поле K конечно над $\mathcal{O}$ и содержит какой-нибудь базис k-векторного пространства K.
2) Если $\mathcal{O}$ - область главных идеалов, то $\mathcal{O}_K$ - свободный $\mathcal{O}$-модуль ранга $n = [K : k]$.
3) $\mathcal{O}_K$ - тоже NICD (доказательство см. в полном конспекте).

Дробные идеалы.

Пусть $\mathcal{O}$ -целостное кольцо, k - поле частных $\mathcal{O}$. Если I и J - $\mathcal{O}$ - подмодули в k, то определены $\mathcal{O}$ - подмодули в k : $I^{-1} \stackrel{\text{def}}{=} \{x \in k \mid xI \subset \mathcal{O}\}$, $\mathcal{O}(I) \stackrel{\text{def}}{=} \{x \in k \mid xI \subset I\}$, $I + J \stackrel{\text{def}}{=} \{x + y,\ x \in I,\ y \in J\}$, $IJ \stackrel{\text{def}}{=} \{\sum x_i y_i$ (конечная сумма), $x_i \in I,\ y_i \in J\}$.

Если I - $\mathcal{O}$ -подмодуль в k, а $\mathfrak{p} \subset \mathcal{O}$ -простой идеал, то $I_{\mathfrak{p}} \stackrel{\mathrm{def}}{=} I\mathfrak{p}$ - $\mathcal{O}_{\mathfrak{p}}$ -подмодуль в k. Если I_0 - идеал в $\mathcal{O}_{\mathfrak{p}}$, то $I_0 \cap \mathcal{O}$ - идеал в $\mathcal{O}$, причем $(I_0 \cap \mathcal{O})_{\mathfrak{p}} = I_0$. Отображение $I_0 \mapsto I_0 \cap \mathcal{O}$ переводит простые идеалы в простые, ненулевые - в ненулевые, нетривиальные - в нетривиальные.

Пусть I - $\mathcal{O}$ -подмодуль в k. Он называется дробным идеалом, если $I \neq \{0\}$ и $I^{-1} \neq \{0\}$.

Теорема (3.12). Если $\mathcal{O}$ - нетерово целостное кольцо, k - его поле частных, и $I \subset k$ - ненулевой $\mathcal{O}$-подмодуль, то I является дробным идеалом $\Leftrightarrow$ он конечно порожден. Если это так, то I^{-1} - тоже дробный идеал, а $\mathcal{O}(I) = \mathcal{O}$. Если I и J - дробные идеалы, то $I + J$, IJ, и $I \cap J$ - тоже дробные идеалы.

Дискретно нормированные кольца и дедекиндовы области.

NICD - кольцо называется дискретно нормированным кольцом (d.v.r.), если оно содержит ровно один ненулевой простой идеал.

Теорема-определение (3.14). Любое d.v.r. $\mathcal{O}$ является областью главных идеалов. Имеется изоморфизм групп $\mathrm{v} : k^*/\mathcal{O}^* \stackrel{\to}{\sim} \mathbf{Z}$ такой, что $||x|| = s^{-\mathrm{v}(x)}$, $(s > 1)$ определяет неархимедово дискретное нормирование поля частных, для которого $\mathcal{O}$ служит кольцом нормирования, а его единственный ненулевой простой идеал $\mathfrak{p}$ - идеалом нормирования. Для дробного идеала $I \subset k$ $\mathrm{v}(I) \stackrel{\mathrm{def}}{=} \inf_{a \in I} \mathrm{v}(a)$ конечно.

Теорема-определение (3.15). NICD - кольцо $\mathcal{O}$ называется дедекиндовой областью, если выполнено одно из эквивалентных условий:
1) все его ненулевые простые идеалы максимальны.
2) Для любого ненулевого простого идеала $\mathfrak{p} \subset \mathcal{O}$ локальное кольцо $\mathcal{O}_{\mathfrak{p}}$ - d.v.r.
3) Для любого дробного $\mathcal{O}$ -идеала $I \subset k$ $I^{-1}I = \mathcal{O}$.

Дробные идеалы в поле частных дедекиндовой области $\mathcal{O}$ образуют группу относительно операций IJ и I^{-1}, свободно порожденную ненулевыми простыми идеалами кольца $\mathcal{O}$. Если определить $\mathrm{v}_{\mathfrak{p}}(I)$ формулой $\mathrm{v}_{\mathfrak{p}}(I) = \inf_{a \in I} \mathrm{v}_{\mathfrak{p}}(a)$, то $I = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(I)}$ (это конечное произведение), при этом $\forall \mathfrak{p}$ $I\mathcal{O}_{\mathfrak{p}} = (\mathfrak{p}\mathcal{O}_{\mathfrak{p}})^{\mathrm{v}_{\mathfrak{p}}(I)}$.

Решетки в конечных сепарабельных расширениях.

Если $N \subset K$ -произвольный $\mathcal{O}$-подмодуль, а $\mathfrak{p} \subset \mathcal{O}$ - простой идеал, определим $N_{\mathfrak{p}} \stackrel{\text{def}}{=} N\mathcal{O}_{\mathfrak{p}}$. Справедлива формула $N = \bigcap\limits_{\mathfrak{p}} N_{\mathfrak{p}}$.

Конечнопорожденный $\mathcal{O}$-подмодуль в K, содержащий некоторый базис k-векторного пространства K называется $\mathcal{O}$-решеткой в K.

Если $\mathcal{O}$ - область главных идеалов, то любая $\mathcal{O}$-решетка - свободный $\mathcal{O}$-модуль ранга n. Если N - $\mathcal{O}$-решетка,то $N_{\mathfrak{p}}$ - $\mathcal{O}_{\mathfrak{p}}$-решетка.

Начиная с этого момента предполагается, что $\mathcal{O}$ - дедекиндова область, k - её поле частных, K/k - конечное сепарабельное расширение, $[K : k] = n$.

Индекс решеток.

$(M : N)_{\mathcal{O}}$ - это $\mathcal{O}$ - дробный идеал в k, который определяется по правилу:
Если M и N - свободные $\mathcal{O}$-модули ранга n, то $(M : N)_{\mathcal{O}} \stackrel{\text{def}}{=} (\det A)$, где A - матрица координат элементов базиса решетки N по отношению к базису решетки M.
В общем случае $(M : N)_{\mathcal{O}} \stackrel{\text{def}}{=} \prod\limits_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}((M_{\mathfrak{p}}:N_{\mathfrak{p}})_{\mathcal{O}_{\mathfrak{p}}})}$.

Свойства индекса:
1) $(M : N)_{\mathcal{O}}(N : T)_{\mathcal{O}} = (M : T)_{\mathcal{O}}$.
2) $(M : M)_{\mathcal{O}} = \mathcal{O}$
3) Пусть $N \subset M$. Тогда $(M : N)_{\mathcal{O}} \subset \mathcal{O}$, равенство выполняется только при $M = N$. Если $\mathcal{O} = \mathbf{Z}$,то идеал $(M : N)_{\mathbf{Z}}$ порождается обычным индексом $(M : N)$.
4) Если $l : K \to K$ - невырожденное k-линейное отображение, то $(l(M) : l(N))_{\mathcal{O}} = (M : N)_{\mathcal{O}}$.
5) Пусть $\mathfrak{p} \subset \mathcal{O}$ - простой идеал. Тогда $(D_{\mathcal{O}}(N))_{\mathfrak{p}} = D_{\mathcal{O}_{\mathfrak{p}}}(N_{\mathfrak{p}})$.

Дуальная решетка и дискриминант.

Если N - произвольный $\mathcal{O}$ -подмодуль в K, то дуальный $\mathcal{O}$-подмодуль $D_{\mathcal{O}}(N) \stackrel{\text{def}}{=} \{y \in K$ такие,что $\forall x \in N \; Tr(xy) \in \mathcal{O}\}$.

Свойства дуальных решеток: пусть N и M - $\mathcal{O}$-решетки в K.
1) Если $N = \langle\{e_i\}\rangle$ - свободный $\mathcal{O}$-модуль ранга n,то $D_{\mathcal{O}}(N)$ - тоже свободный модуль ранга n, порожденный дуальным базисом $\{f_j\}$.
2) $D_{\mathcal{O}}(N)$ - тоже $\mathcal{O}$-решетка.
3) $D_{\mathcal{O}}(D_{\mathcal{O}}(N)) = N$.
4) $(D_{\mathcal{O}}(N) : D_{\mathcal{O}}(M))_{\mathcal{O}} = (M : N)_{\mathcal{O}}$.
5) Пусть $\mathfrak{p} \subset \mathcal{O}$ -простой идеал. Тогда $(D_{\mathcal{O}}(N))_{\mathfrak{p}} = D_{\mathcal{O}_{\mathfrak{p}}}(N_{\mathfrak{p}})$.

Дискриминант $\mathcal{O}$-решетки N - это дробный $\mathcal{O}$-идеал в k, задаваемый формулой $\mathfrak{d}_{\mathcal{O}}(N) \stackrel{\text{def}}{=} (D_{\mathcal{O}}(N) : N)_{\mathcal{O}}$. Вместо $\mathfrak{d}_{\mathcal{O}}(\mathcal{O}_K)$ часто пишут $\mathfrak{d}_{K/k}$, это целый идеал в $\mathcal{O}$.

Свойства дискриминанта: пусть N и M - $\mathcal{O}$-решетки в K.
1) Если $N = \langle\{e_i\}\rangle$ - свободный $\mathcal{O}$-модуль,то $\mathfrak{d}_{\mathcal{O}}(N) = (\det Tr(e_i e_j))$.
2) $\mathfrak{d}_{\mathcal{O}}(N) = \mathfrak{d}_{\mathcal{O}}(M)(M : N)^2_{\mathcal{O}}$.
3) Пусть $N \subset M$. Тогда $\mathfrak{d}_{\mathcal{O}}(N) \subset \mathfrak{d}_{\mathcal{O}}(M)$, равенство выполняется только при $M = N$.
4) $\mathfrak{d}_{\mathcal{O}}(N) = \prod\limits_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{d}_{\mathcal{O}_{\mathfrak{p}}}(N_{\mathfrak{p}}))}$.

Если N - свободный $\mathcal{O}$-модуль,то формула 1) определяет элемент $\Delta_{\mathcal{O}}(N) \in k^*/(\mathcal{O}^*)^2$, порождающий $\mathfrak{d}_{\mathcal{O}}(N)$. При $\mathcal{O} = \mathbf{Z}$ используют обозначение $\Delta(N) \in \mathbf{Q}$ (а при $N = \mathcal{O}_K$ - обозначение $\Delta_K \in \mathbf{Z}$).

Идеалы в $\mathcal{O}$ и идеалы в $\mathcal{O}_K$.

Говорят, что простой идеал $\mathfrak{P} \subset \mathcal{O}_K$ лежит над простым идеалом $\mathfrak{p} \subset \mathcal{O}$ (или $\mathfrak{P} \,|\, \mathfrak{p}$), если $\mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$.

Теорема (3.27). 1) $\mathcal{O}_K$ - дедекиндова область.
2) Пусть $\mathfrak{p} \subset \mathcal{O}$ -простой идеал. Тогда $(\mathcal{O}_K)_{\mathfrak{p}}(\stackrel{\text{def}}{=} \mathcal{O}_K\mathcal{O}_{\mathfrak{p}})$ - целое замыкание $\mathcal{O}_{\mathfrak{p}}$ в K.
3) Для любого простого идеала $\mathfrak{p} \subset \mathcal{O}$ существует простой идеал $\mathfrak{P} \subset \mathcal{O}_K$ (не обязательно единственный) такой, что $\mathfrak{P} \,|\, \mathfrak{p}$. Обратно, если $\mathfrak{P} \subset \mathcal{O}_K$ - ненулевой простой идеал, то $\mathfrak{P} \cap \mathcal{O} \neq (0)$.

Дифферентой $\mathfrak{D}$ или $\mathfrak{D}_{K/k}$ называется идеал в $\mathcal{O}_K$, определенный формулой $\mathfrak{D} \stackrel{\text{def}}{=} (D_{\mathcal{O}}(\mathcal{O}_K))^{-1}$ (определение корректно, поскольку $\mathcal{O}$-решетка $D_{\mathcal{O}}(\mathcal{O}_K)$ является $\mathcal{O}_K$ - дробным идеалом в K, содержащим $\mathcal{O}_K$).

Теорема (3.29). Пусть $x \in \mathcal{O}_K$ - примитивный элемент (т.е. $K = k(x)$), $P_x \in \mathcal{O}[T]$ - его минимальный полином.Тогда
1) $\mathcal{O}[x]$ - $\mathcal{O}$ -решетка в K.
2) $D_{\mathcal{O}}(\mathcal{O}[x]) = (P'(x))^{-1}\mathcal{O}[x]$.
3) $\mathfrak{d}_{\mathcal{O}}(\mathcal{O}[x]) = (N_{K/k}(P_x'(x))) = (\Delta_{P_x})$.
4) $\mathcal{O}_K = \mathcal{O}[x] \Leftrightarrow \mathfrak{D}_{K/k} = (P_x'(x))$.

p-адическое разложение расширения K/k.

Теорема (3.30). Пусть K/k - конечное расширение полей, $||||$:$K \to \mathbf{R}_{\geq 0}$ -нормирование, ограничение которого на k превращает k в полное метрическое пространство.Тогда топология пространства K в метрике, определяемой нормированием $||\,||$, совпадает с топологией координатного пространства.

Тем самым, продолжение нормирования с полного поля k на на его конечное расширение K, если оно существует, определено однозначно.

Пусть $\mathcal{O}$ - дедекиндова область, k - её поле частных, $\mathfrak{p} \subset \mathcal{O}$ - ненулевой простой идеал, $\mathcal{O}_{\mathfrak{p}} \subset k$ -соответствующее локальное кольцо, $\widehat{k_{\mathfrak{p}}}$ - пополнение поля k по отношению к p-адическому нормированию $||\,||_{\mathfrak{p}}$ (определенному при помощи функции $\mathrm{v}_{\mathfrak{p}}$), $\widehat{\mathcal{O}_{\mathfrak{p}}}$ - топологическое замыкание $\mathcal{O}_{\mathfrak{p}}$ в $\widehat{k_{\mathfrak{p}}}$, K/k - конечное сепарабельное расширение степени n, $\mathcal{O}_K$ - целое замыкание $\mathcal{O}$ in K.

Положим $\mathbf{V}_{\mathfrak{p}} \overset{\text{def}}{=} K \otimes_k \widehat{k_{\mathfrak{p}}}$, фиксируем изоморфизм $\mathbf{V}_{\mathfrak{p}} \simeq \oplus K_i$, где K_i/k - сепарабельные расширения степеней n_i (набор их классов изоморфизма определен однозначно с точностью до перестановки), и снабдим $\mathbf{V}_{\mathfrak{p}}$ топологией n - мерного координатного пространства над $\widehat{k_{\mathfrak{p}}}$. Эта топология не зависит от выбора изоморфизма $\mathbf{V}_{\mathfrak{p}} \simeq \oplus K_i$, и $\mathbf{V}_{\mathfrak{p}}$ превращается в топологическую $\widehat{k_{\mathfrak{p}}}$ - алгебру. Проекции $\mathbf{V}_{\mathfrak{p}} \to K_i$ (и их ограничения на K) будем обозначать π_i.

Теорема (3.31). Имеется взаимнооднозначное соответствие между тремя множествами:
1) Различные простые идеалы $\mathfrak{P}_i \subset \mathcal{O}_K$, лежащие над $\mathfrak{p} \subset \mathcal{O}$,
2) Различные нормирования $||||: K \to \mathbf{R}_{\geq 0}$, продолжающие $\mathfrak{p}$-адическое нормирование на k,
3) Компоненты K_i прямой суммы $\mathbf{V}_{\mathfrak{p}} = \oplus K_i$.

Если фиксировать алгебраическое замыкание $\overline{\widehat{k_\mathfrak{p}}}/\widehat{k_\mathfrak{p}}$ и отождествить $\overline{k}$ с его подполем, состоящим из элементов, алгебраических над k, то естественное отображение $\sigma \mapsto \sigma \circ \pi_i$ установит взаимнооднозначное соответствие $\bigcup \Sigma_{K_i/\widehat{k_\mathfrak{p}}}^{\overline{\widehat{k_\mathfrak{p}}}/\widehat{k_\mathfrak{p}}} \xrightarrow{\sim} \Sigma_{K/k}^{\overline{k}/k}$.

Теорема (3.33). Предположим, что K/k - расширение Галуа. Пусть $G = \mathrm{Gal}\,(K/k)$. Тогда

1) G транзитивно действует на множестве идеалов $\mathfrak{P}_i \mid \mathfrak{p}$. Все показатели степени в произведении $\mathfrak{p}\mathcal{O}_K = \prod \mathfrak{P}_i^{e_i}$ одинаковы.

2) Стационарная подгруппа идеала относительно действия G (т.е. $G_\mathfrak{P} \overset{\mathrm{def}}{=} \{g \in G$ такие,что $g\mathfrak{P} = \mathfrak{P}\}$) называется подгруппой разложения идеала $\mathfrak{P}$. Подгруппы $G_{\mathfrak{P}_i}$ сопряжены.

3) $K_i = \pi_i(K)\widehat{k_\mathfrak{p}}$, все расширения $K_i/\widehat{k_\mathfrak{p}}$ изоморфны друг другу и являются расширениями Галуа, $\mathrm{Gal}\,(K_i/\widehat{k_\mathfrak{p}}) \simeq G_{\mathfrak{P}_i}$.

Решетки в K и решетки в $\mathbf{V}_\mathfrak{p}$.

Определим $\widehat{\mathcal{O}}_\mathfrak{p}$ - решетку в $\mathbf{V}_\mathfrak{p}$ как свободный $\widehat{\mathcal{O}}_\mathfrak{p}$ - подмодуль ранга n (напомним,что $\widehat{\mathcal{O}}_\mathfrak{p}$ - область главных идеалов). Индекс решеток определяется, как и раньше (это $\widehat{\mathcal{O}}_\mathfrak{p}$ - дробный идеал в $\widehat{k_\mathfrak{p}}$).
Если M - $\mathcal{O}$ - решетка в K, то $M\widehat{\mathcal{O}}_\mathfrak{p}$ - $\widehat{\mathcal{O}}_\mathfrak{p}$ - решетка в $\mathbf{V}_\mathfrak{p}$.
Билинейная форма $Tr_{K/k}(ab)$ может быть продолжена с K на $\mathbf{V}_\mathfrak{p}$ по $\widehat{k_\mathfrak{p}}$-линейности, обозначим это продолжение $\langle\, ,\, \rangle$. Имеет место формула $\langle a, b\rangle = \sum Tr_{K_i/\widehat{k_\mathfrak{p}}}(\pi_i(a)\pi_i(b))$.
Использование формы $\langle\, ,\, \rangle$ позволяет определить двойственную $\widehat{\mathcal{O}}_\mathfrak{p}$ - решетку и дискриминант.

Теорема. Пусть M, N - $\mathcal{O}$ - решетки в K. Тогда
1) $(M : N)_\mathcal{O}\widehat{\mathcal{O}}_\mathfrak{p} = (M\widehat{\mathcal{O}}_\mathfrak{p} : N\widehat{\mathcal{O}}_\mathfrak{p})_{\widehat{\mathcal{O}}_\mathfrak{p}}$.
2) $D_\mathcal{O}(N)\widehat{\mathcal{O}}_\mathfrak{p} = D_{\widehat{\mathcal{O}}_\mathfrak{p}}(N\widehat{\mathcal{O}}_\mathfrak{p})$.
3) $\mathfrak{d}_\mathcal{O}(N)\widehat{\mathcal{O}}_\mathfrak{p} = \mathfrak{d}_{\widehat{\mathcal{O}}_\mathfrak{p}}(N\widehat{\mathcal{O}}_\mathfrak{p})$.

Назовем $\widehat{\mathcal{O}}_\mathfrak{p}$ - решетку M в $\mathbf{V}_\mathfrak{p} = \oplus K_i$ разложимой, если $M = \oplus \pi_i(M)$.

Теорема. Пусть M и N - разложимые $\widehat{\mathcal{O}}_\mathfrak{p}$ - решетки в $\mathbf{V}_\mathfrak{p}$. Тогда
1) $(M : N)_{\widehat{\mathcal{O}}_\mathfrak{p}} = \prod (\pi_i(M) : \pi_i(N))_{\widehat{\mathcal{O}}_\mathfrak{p}}$.
2) $D_{\widehat{\mathcal{O}}_\mathfrak{p}}(N) = \oplus D_{\widehat{\mathcal{O}}_\mathfrak{p}}(\pi_i(N))$.
3) $\mathfrak{d}_{\widehat{\mathcal{O}}_\mathfrak{p}}(N) = \prod \mathfrak{d}_{\widehat{\mathcal{O}}_\mathfrak{p}}(\pi_i(N))$.

Разложимость дробных идеалов и гомоморфизм нормы.

Нормой $\mathcal{O}_K$ - дробного идеала в K называется $\mathcal{O}$ - дробный идеал в k, задаваемый формулой $N_{K/k}(I) \stackrel{\mathrm{def}}{=} (\mathcal{O}_K : I)_{\mathcal{O}}$.

$\mathfrak{p}$ - адическое нормирование однозначно продолжается с $\widehat{k_\mathfrak{p}}$ на K_i (ибо $\widehat{k_\mathfrak{p}}$ полно), и определено кольцо нормирования $\mathcal{O}_i \stackrel{\mathrm{def}}{=} \{x \in K_i$ такие, что $||x|| \le 1\}$. $\mathcal{O}_i$ совпадает с целым замыканием $\widehat{\mathcal{O}}_\mathfrak{p}$ в K_i и с проекцией $\pi_i(\mathcal{O}_K\widehat{\mathcal{O}}_\mathfrak{p})$.

Теорема. Пусть I- $\mathcal{O}_K$ - дробный идеал в K. Тогда
1) $\widehat{\mathcal{O}}_\mathfrak{p}$ - решётка $I\widehat{\mathcal{O}}_\mathfrak{p}$ разложима. В частности, $\mathcal{O}_K\widehat{\mathcal{O}}_\mathfrak{p} = \oplus\mathcal{O}_i$.
2) $N_{K/k}(I)\widehat{\mathcal{O}}_\mathfrak{p} = \prod N_{K_i/\widehat{k_\mathfrak{p}}}(\pi_i(I)\mathcal{O}_i)$.
3) $N_{K/k} : \mathcal{F}(\mathcal{O}_K) \to \mathcal{F}(\mathcal{O})$ - гомоморфизм групп.
4) $\pi_i(\mathfrak{D}_{K/k})\mathcal{O}_i = \mathfrak{D}_{K_i/\widehat{k_\mathfrak{p}}}$.
5) $\mathfrak{d}_{K/k}\widehat{\mathcal{O}}_\mathfrak{p} = \prod \mathfrak{d}_{K_i/\widehat{k_\mathfrak{p}}}$.
6) $N_{K/k}(\mathfrak{D}_{K/k}) = \mathfrak{d}_{K/k}$.

Вычисление кольца $\mathcal{O}_K$.

Пусть $\mathcal{O} = \mathbf{Z}$ (будем опускать индекс $_\mathbf{Z}$), $K = K(x)$, где x - корень минимального полинома $P_x = T^n + a_{n-1}T^{n-1} + \cdots + a_0$, причем все $a_i \in \mathbf{Z}$. Предположим, что $[K : \mathbf{Q}] = n$ (т.е. x примитивен). Индекс решетки $\mathbf{Z}[x]$ в $\mathcal{O}_K$ ограничен сверху квадратным корнем из максимального квадрата, делящего Δ_{P_x}.

Например, если $P_x = T^2 - d$, где d свободно от квадратов, то $\Delta_x = 4d$, и либо $\Delta_K = 4d$ (тогда индекс равен 1), либо $\Delta_K = d$ (тогда индекс равен 2). Оба случая встречаются (при $d \equiv 2$ bkb $3 \mod 4$ и при $d \equiv 1 \mod 4$ соответственно).

Поскольку множество решеток Λ с ограниченным индексом $(\Lambda : \mathbf{Z}[x])$ конечно и их базисы могут быть явно выписаны, то можно выбрать решетку, все элементы базиса которой - целые алгебраические числа, имеющую наименьший дискриминант. Это и будет решетка $\mathcal{O}_K$.

Теорема (3.39). Пусть P_x - полином Эйзенштейна по отношению к простому числу p. Тогда $p \nmid (\mathcal{O}_K : \mathbf{Z}[x])$.

Пример. Пусть $P_x = T^3 - 2$. Тогда P_x 2-Эйзенштейнов, а P_{x-2} 3-Эйзенштейнов. Поскольку $\Delta_{P_x} = -108$, решётка $\mathbf{Z}[x]$ (она же $\mathbf{Z}[x-2]$) совпадает с $\mathcal{O}_K$.