Пусь, как и предыдущей лекции, $K \subset L$ — расширение числовых полей, $\mathcal{O}_K$ и $\mathcal{O}_L$ — их кольца целых; и пусть теперь $K \subset L$ — расширение Галуа с группой Галуа G.

Теорема. Пусть $\mathfrak{p}$ — максимальный идеал в кольце $\mathcal{O}_K$. $\mathfrak{p}\mathcal{O}_K = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_n^{e_n}$ — разложенике на простые множители. Тогда G транзитивно действует на множестве идеалов $\{\mathfrak{B}_i\}$.

Упражнение 9.1. Докажите, что кольцо $\mathcal{O}_L$ инвариантно относительно действия группы G.

Упражнение 9.2. Докажите, Китайскую теорему об остатках, т.е., что для любого кольца A, и для любого набора идеалов $I_1, \dots, I_n$ кольца A, если $I_k + I_l = A$ при вех i и j, то $A/(I_1 \dots I_n) = A/I_1 \sum \dots \sum A/I_n$.

Упражнение 9.3. Докажите, что $e_1 = \dots = e_n$,и, что $\mathcal{O}_L/\mathfrak{B}_1 \cong \dots \cong \mathcal{O}_L/\mathfrak{B}_n$.

Упражнение 9.4. Пусть $\mathfrak{p}$ — простой идеал кольца $\mathcal{O}_K$, $\mathfrak{B}$ — пhостой идеал кольца $\mathcal{O}_L$, лежащий над $\mathfrak{p}$. Докажите, что расширение полей $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{B}$ является расширением Галуа.

Теорема. Пусть $\mathfrak{p}$ — простой идеал кольца $\mathcal{O}_K$, $\mathfrak{B}$ — постой идеал кольца $\mathcal{O}_L$, лежащий над $\mathfrak{p}$ в котором расширение полей $K \subset L$ не разветвлено. Тогда канонический гомоморфизм $\varphi : G_{\mathfrak{B}} \to Gal(\mathcal{O}_L/\mathfrak{B}, \mathcal{O}_K/\mathfrak{p})$ является изоморфизмом.

Упражнение 9.5. Не используя последнюю теорему докажите, что $|G_{\mathfrak{B}}| = |Gal(\mathcal{O}_L/\mathfrak{B}, \mathcal{O}_K/\mathfrak{p})|$.

Определение. Прообраз морфизма Фробениуса приотображении φ называется элементом Фробениуса группы Галуа G.

Упражнение 9.6. Докажите, что элемент Фробениуса определен с точностью до сопряжения, и, в частности, если группа G коммутативна, то элемент Фробениуса определен однозначно.

Определение. Рассмотрим билинейную форму $tr(uv)$ на L. Пусть A — подгруппа аддитвной группы поля L. Тогда $A' = \{z \in L | Tr(Az) \subset \mathcal{O}_K\}$

Упражнение 9.7. Докажите, что если I — дробный идеал, то I' тоже дробный идеал.

Определение. Дифферентой расширения полей $K \subset L$ называется дробный идеал $\mathcal{O}_L'^{-1}$.

Определение. Пусть I — идеал в кольце $\mathcal{O}_L$. Нормой I называется идеал N_I в кольце $\mathcal{O}_K$, порожденный множеством $\{N_\alpha | \alpha \in I\}$.

Теорема. Дискриминант равен норме дифференты.

Упражнение 9.8. Пусть $\mathfrak{p}$ — идеал кольца $\mathcal{O}_K$, и пусть идеал $\mathfrak{B}$ кольца $\mathcal{O}_L$ лежит над $\mathfrak{p}$. Докажите, что $N_{\mathfrak{B}} = \mathfrak{p}^{[\mathcal{O}_L/\mathfrak{B}:\mathcal{O}_K/\mathfrak{p}]}$.

Упражнение 9.9. Докажите, последнюю теорему в случае $K = \mathbb{Q}$.

Везде далее $K = \mathbb{Q}(\zeta)$, где ζ — первообразный корень из 1 степени m.

Упражнение 9.10. В каких точках ветвится поле K?

Упражнение 9.11. Пусть $m = p^r$. Докажите, что $(p) = \mathfrak{B}^e$ — разложение на простые множители в кольце $\mathcal{O}_K$.

Указание. Пусть $f = (1-x^m)/(1-x)$. Тогда $p = f(1) = \prod\limits_{t:(t,p)=1} (1-\zeta)^t$

Упражнение 9.12. Докажите, что $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Указание. Используйте упражнения 8.16 и 8.17.

Упражнение 9.13. Найдите кольцо целых поля K для призвольного знаения m.

Указание. Пусть $m = m_1 m_2$. Тогда $K = \mathbb{Q}(\zeta_{m_1}) \otimes \mathbb{Q}(\zeta_{m_2})$, и $D_K = D_{\mathbb{Q}(\zeta_{m_1})} D_{Q(\zeta m_2)}$.