Лекция 10. Квадратичный закон взаимности и морфизм Фробениуса.

Под занавес мы докажем *квадратичный закон взаимности.* Существует множество доказательств этого утверждения. Наше будет основано на его связи со свойствами морфизма Фробениуса. Это наблюдение является первым шагом при построении теории полей классов, которая изучает абелевы расширения полей и содержит далекое обобщение квадратичного закона взаимности — *закон взаимности Артина.*

Рассмотрим целое число n и простое число p.

Определение. *Символом Лежандра* называется число $\left(\frac{n}{p}\right)$, определяемое следующим образом:

$$\left(\frac{n}{p}\right) = (\overline{n})^{\frac{p-1}{2}} \in \{1, -1\},$$

где $\overline{n}$ — остаток от n при делении на p. Заметим, что это выражение мультипликативно по $\overline{n}$ (то есть уважает умножение). Главное свойство символа Лежандра заключается в том, что $\left(\frac{n}{p}\right)$ равно -1, если n не является квадратом по модулю p, равно 1, если n является ненулевым квадратом по модулю p, и равно 0, если n делится на p.

Квадратичный закон взаимности. Пусть p и q два простых числа, отличных от 2. Тогда

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Сразу будем считать, что $p \neq q$. Рассмотрим расширение $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p})$. Оно не ветвится над q и, как мы уже видели, идеал (q) остается простым в $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p})$, то есть $f = 2$, тогда и только тогда, когда в $\mathbb{F}_q$ нет квадратного корня из $p(\mathrm{mod} q)$, что равносильно тому, что $\left(\frac{p}{q}\right) = -1$. Связать это с морфизмом Фробениуса нам поможет следующее очевидное, но важное

Утверждение 10.1. Пусть L/K абелево расширение Галуа глобальных полей, то есть полей частных дедекиндовых колец $\mathcal{O}_K$ и $\mathcal{O}_L$, не ветвящееся над простым идеалом $\mathfrak{p} \subset \mathcal{O}_K$. Тогда порядок морфизма Фробениуса $\mathrm{Fr}_\mathfrak{p}$ равен $f = [\mathcal{O}_L/\mathfrak{B} : \mathcal{O}_K/\mathfrak{p}]$, где $\mathfrak{B} \subset \mathcal{O}_L$ — произвольный простой идеал, "висящий" над $\mathfrak{p}$.

Стало быть, $\left(\frac{p}{q}\right) = \mathrm{Fr}_q \in \mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) \cong \{1, -1\}$.

Для вычисления морфизма Фробениуса, вложим наше расширение в круговое.

Утверждение 10.2. Пусть $\mathbb{Q} \subset K \subset L$ башня конечных абелевых расширений $\mathbb{Q}$, $\mathbb{Z} \subset \mathcal{O}_K \subset \mathcal{O}_L$ соответствуюшее расширение колец целых, а $(p) \subset \mathfrak{p} \subset \mathfrak{B}$ — "висящие" друг над другом идеалы в этих кольцах. Тогда при естественном гомоморфизме $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ морфизм Фробениуса $\mathrm{Fr}_{p,L} \in \mathrm{Gal}(L/\mathbb{Q})$, построенный по паре $(p) \subset \mathfrak{B}$, переходит в морфизм Фробениуса $\mathrm{Fr}_{p,K} \in \mathrm{Gal}(K/\mathbb{Q})$, построенный по паре $(p) \subset \mathfrak{p}$.

Доказательство. Утверждение следует из коммутативности диаграммы:

$$\begin{array}{ccccccc}
\mathrm{Gal}(L/\mathbb{Q}) & \longleftarrow & G_{\mathfrak{B}} & = & <\mathrm{Fr}_{p,L}> & \longrightarrow & \mathrm{Gal}((\mathcal{O}_L/\mathfrak{B})/\mathbb{F}_p) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathrm{Gal}(K/\mathbb{Q}) & \longleftarrow & G_{\mathfrak{p}} & = & <\mathrm{Fr}_{p,K}> & \longrightarrow & \mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)
\end{array}$$

Добавим лишь то, что при отображении $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{B})/\mathbb{F}_p) \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ "настоящий" морфизм Фробениуса остается самим собой.

Докажем теперь, что есть вложение в круговое поле.

Утверждение 10.3. $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_N)$, где $N = p$, если $p \equiv 1(\mathrm{mod}4)$, и $N = 4p$, если $p \equiv 3(\mathrm{mod}4)$.

Доказательство. Рассмотрим аддитивный характер (то есть гомоморфизм) $\mathbb{F}_p \to S^1$, при котором $i \mapsto \zeta_p^i$, и его скалярное произведение с мультипликативным характером $i \mapsto \left(\frac{i}{p}\right)$:

$$\alpha = \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \zeta_p^i.$$

Это выражение называется Гауссовой суммой (обратите внимание, что подобным образом, но только для поля $\mathbb{R}$, а не $\mathbb{F}_p$, определяется Г-функция). Посчитаем его квадрат:

$$\alpha^2 = \sum_{k=0}^{p-1} \left(\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \left(\frac{k-i}{p}\right) \right) \zeta_p^k.$$

При $k = 0$

$$\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \left(\frac{-i}{p}\right) = \left(\frac{-1}{p}\right)(p-1).$$

При $k \neq 0$ имеем

$$\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \left(\frac{i}{p}\right) \left(\frac{k/i-1}{p}\right) = \sum_{j=0}^{p-2} \left(\frac{j}{p}\right) = -\left(\frac{-1}{p}\right),$$

так как сумма всех сиволов Лежандра равна 0 (квадратичных вычетов и невычетов поровну!). Итак, учитывая, что сумма всех корней p-ой степени из 1 равна 0, получаем

$$\alpha^2 = \left(\frac{-1}{p}\right)(p-1) - \left(\frac{-1}{p}\right)\sum_{k=0}^{p-1}\zeta_p^k = \left(\frac{-1}{p}\right)p = (-1)^{\frac{p-1}{2}}p.$$

Таким образом, при $p \equiv 1(\mathrm{mod} 4)$ мы доказали, что $\alpha^2 = p$, а значит $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$. При $p \equiv 3(\mathrm{mod} 4)$ мы имеем, что $(i\alpha)^2 = p$, и $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p, i) = \mathbb{Q}(\zeta_{4p})$.

На самом деле, утверждение 10.3 является частным случаем очень важной теоремы.

Теорема Кронекера-Вебера. Любое абелево расширение $\mathbb{Q}$ вкладывается в круговое поле $\mathbb{Q}(\zeta_N)$ для подходящего N.

Вложение в круговое поле очень удобно для вычисления действия морфизма Фробениуса. Напомним, что $\mathrm{Fr}_q(\zeta_N) = \zeta_N^p$. Значит,

$$\mathrm{Fr}_q(\alpha) = (-1)^{\frac{p-1}{2}}\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\zeta_p^{iq} = \sum_{j=0}^{p-1}\left(\frac{q}{p}\right)\left(\frac{j}{p}\right)\zeta_p^j = \left(\frac{q}{p}\right)\alpha,$$

$$\mathrm{Fr}_q(i) = (-1)^{\frac{q-1}{2}}i.$$

Учитывая, что в то же время $\mathrm{Fr}_q(\sqrt{p}) = \left(\frac{p}{q}\right)\sqrt{p}$, получаем квадратичный закон взаимности.

Сформулируем теперь одну важную теорему про морфизм Фробениуса.

Пусть $K/\mathbb{Q}$ — произвольное расширение Галуа, $M \subset \mathrm{Gal}(K/\mathbb{Q})$ — инвариантное относительно сопряжений подмножество. Естественно спросить, насколько часто для простого числа p выполняется то, что $\overline{\mathrm{Fr}_p} \subset M$, где $\overline{\mathrm{Fr}_p}$ — класс сопряженности, содержащий соответствующий морфизм Фробениуса. Обозначим это множество простых чисел через $\mathrm{Fr}^{-1}(M)$.

Определение. *Плотностью* подмножества S множества всех простых чисел P называется, если он существует, следующий предел

$$\rho(S) = \lim_{N\to\infty}\frac{|\{p \in S | p < N\}|}{|\{p \in P | p < N\}|}.$$

Теорема плотности Чеботарева. $\rho(\mathrm{Fr}^{-1}(M)) = \frac{|M|}{|\mathrm{Gal}(K/\mathbb{Q})|}$.

Это утверждение является одним из самых сложных в теории полей классов.

В частности, из него следует, что в абелевом расширении для любого элемента из группы Галуа существует бесконечно много простых чисел с данным морфизмом Фробениуса.

В частном случе, когда $K = \mathbb{Q}(\zeta_n)$, это утверждение превращается в классическую теорему Дирихле:

Теорема Дирихле о прогрессии. В арифметической прогрессии со взаимно простыми начальным членом и разностью, существует бесконечно много простых чисел.