Квадратичный закон взаимности

Часть 27. Ветвление и степень идеала.

Пусть $F:\mathbb{Q}$ — расширение степени n, а $P\subset A\subset F$ — простой идеал кольца целых. Пересечение $P\cap\mathbb{Z}$ является простым идеалом в $\mathbb{Z}$, т.е. $P\cap\mathbb{Z}$ порождено каким-то простым числом p. Рассмотрим соответствующий идеал $(p)\subset A$.

Определение. Индексом ветвления идеала P называется число $\mathrm{ord}_P(p)=:e_P$.

Терминология и вся интуиция просходят из аналогии с кольцом многочленов $\mathbb{C}[t]$. Расширение колец $\mathbb{C}[t]\hookrightarrow\mathbb{C}[z]=A'$, где $t=z^n$ отвечает отображению из комплексной прямой $\mathbb{A}^1$ с координатой z в комплексную прямую $\mathbb{A}^1$ с координатой t. Это отображение вне нуля является неразветвленным накрытием степени n, а в нуле имеет ветвление индекса n. Соответственно, идеал $(t)\subset A'$ является n-ой степенью простого идеала $(z)\subset A'$. А любой другой идеал $(t-\lambda)\subset A'$ распадается в произведение n *различных* простых идеалов кольца A'.

Определение. Степенью простого идеала $P\subset A$ называется степень поля A/P над простым полем $\mathbb{F}_p$: $f_P=\deg P:=[A/P:\mathbb{F}_p]$. Иначе говоря, $A/P\simeq\mathbb{F}_q$, где $q=p^{f_P}$.

Например, так как квадратный корень из -1 не извлекается в $\mathbb{F}_3=\mathbb{Z}/3\mathbb{Z}$, имеем $\mathbb{Z}[i]/(3)=\mathbb{F}_9$, т.е. степень простого идеала (3) в кольце гауссовых чисел равняется 2.

Теорема. Пусть $(p)=P_1^{e_1}\dots P_k^{e_k}$ — разложение главного идеала (p) в произведение простых. Тогда $\sum e_if_i=n=[F:\mathbb{Q}]$, где $f_i=f_{P_i},\ e_i=e_{P_i}$.

Геометрический аналог этой теоремы гласит, что для любого отображения (разветвленного накрытия) $\mathbb{A}^1 \to \mathbb{A}^1$ число прообразов любой точки, взятых с кратностью, равной индексу ветвления, равно степени этого накрытия. Геометрический аналог очевиден, а формулируется он проще потому, что степени всех простых идеалов равны единице (так как поле $\mathbb{C}$ алгебраически замкнуто).

Для начала докажем Китайскую Теорему об остатках:

Китайская Теорема. Пусть $I_1, \dots, I_k \subset A$ — попарно взаимно простые идеалы, т.е. $I_i + I_j = A\ \forall i \neq j$. Положим $I = I_1 \dots I_k$. Тогда $A/I \simeq A/I_1 \oplus \dots \oplus A/I_k$.

Доказательство: Определим отображение $\psi : A \to A/I_1 \oplus \dots \oplus A/I_k$, $\alpha \mapsto (\alpha \pmod{I_1}, \dots, \alpha \pmod{I_k})$. Докажем его сюръективность. Мы должны проверить, что для любых $\alpha_1, \dots, \alpha_k \in A$ найдется $\alpha \in A$ такое, что $\alpha \equiv \alpha_i \pmod{I)_i}$. Достаточно построить $\beta_i \equiv 1 \pmod{I_i}$, $\beta \equiv 0 \pmod{I)_j}$, $j \neq i$, и потом взять $\alpha = \sum \alpha_i \beta_i$. Построим $\beta = \beta_1$.

Из равенства $(I_1 + I_2) \dots (I_1 + I_k) = A$, раскрывая скобки, получаем $I_1 + I_2 \dots I_k = A$. Значит, найдутся $x \in I_2 \dots I_k$, $y \in I_1$ такие, что $x + y = 1$. Положим $\beta = x$. Итак, сюръективность ψ доказана. Очевидно, ядро $\mathrm{Ker}\psi = I_1 \cap \dots \cap I_k$. Мы должны проверить, что $\mathrm{Ker}\psi = I_1 \cap \dots \cap I_k = I_1 \dots I_k = I$. Тогда получится, что ψ индуцирует искомый изоморфизм $A/I \widetilde{\longrightarrow} A/I_1 \oplus \dots \oplus A/I_k$.

Мы будем рассуждать по индукции по числу идеалов k. Так как мы уже видели, что идеалы I_1 и $J := I_2 \dots I_k$ взаимно просты, достаточно проверить, что $I_1 \cap J = I_1 J$. Во всяком случае, очевидно, $I_1 J \subset I_1 \cap J$. Проверим обратное включение. Для этого выберем $x \in J$, $y \in I_1$, как выше. Пусть $z \in I_1 \cap J$. Тогда $z = z \cdot 1 = zx + zy$. Первое слагаемое лежит в $I_1 J$, а второе — в $J I_1$. Значит, $z \in I_1 J$. $\square$

Лемма. Пусть $P \subset A$ — простой идеал, и $\sharp A/P = p^f$. Тогда $\sharp A/P^e = p^{fe}$.

Доказательство: Индукция по e: так как $\sharp A/P^e = \sharp A/P^{e-1} \cdot \sharp P^{e-1}/P^e$, достаточно проверить, что $\sharp P^{e-1}/P^e = p^f$. Для этого установим изоморфизм между A/P и P^{e-1}/P^e. Выберем $\alpha \in P^{e-1}$ т.ч. $\alpha \notin P^e$. Тогда $P^{e-1} = (\alpha)+P^e$. В самом деле, так как идеал $(\alpha)+P^e$ содержит P^e, он обязан являться какой-то степенью идеала P. Так как он строго содержит P^e и содержится в P^{e-1}, он обязан совпадать с P^{e-1}.

Теперь определим отображение $\phi : A \to P^{e-1}/P^e$, $\beta \mapsto \alpha\beta \pmod{P}^e$. Так как $P^{e-1} = (\alpha) + P^e$, это отображение сюръективно. Его ядро равно P (из однозначности разложения на простые множители в идеалах), а значит, ϕ индуцирует искомый изоморфизм $A/P \xrightarrow{\sim} P^{e-1}/P^e$. $\square$

Теперь вернемся к доказательству Теоремы. Напомним, что $\sharp A/(p) = p^n$ (см. предыдущую лекцию: если $\omega_1, \dots, \omega_n$ — базис A над $\mathbb{Z}$, то $\{\, a_1\omega_1 + \ldots + a_n\omega_n,\ 0 \leqslant a_i < p \,\}$ образуют полную систему представителей для $A/(p)$). Так как идеалы $I_1 = P_1^{e_1}, \dots, I_k = P_k^{e_k}$ взаимно просты, по Китайской Теореме получаем $A/(p) = \bigoplus_i A/P_i^{e_i}$, откуда $p^n = \prod_i p^{e_i f_i}$, т.е. $\sum_i e_i f_i = n$. $\square$

Пусть теперь $F : \mathbb{Q}$ — расширение Галуа, $G = \mathrm{Gal}(F : \mathbb{Q})$. Группа Галуа G действует на кольце A и переводит идеалы в идеалы, сохраняя понятия простоты и делимости. Главный идеал (p) инвариантен относительно действия группы G, следовательно, его простые делители P_i переставляются действием G.

Предложение. Если простые идеалы P_0, P_1 делят (p), то найдется элемент $h \in G$ т.ч. $h(P_1) = P_0$.

Доказательство: От противного. Пусть $P_1, \dots, P_g$ — все простые идеалы, получающиеся из P_1 действием G, и пусть $P_0 \neq P_i$, $i > 0$. Так как P_0 и $P_1 \dots P_g$ взаимно просты, найдется $\alpha \in A \mid \alpha \equiv 0 \pmod{P_0}$, $\alpha \equiv 1 \pmod{P_1 \dots P_g}$. Тогда норма $N_{F:\mathbb{Q}}(\alpha) \in P_0 \cap \mathbb{Z} = (p)$, т.е. $h_1(\alpha) \dots h_n(\alpha)$ делится на p. Значит, $h_1(\alpha) \dots h_n(\alpha)$ лежит в простом идеале P_1, а значит, один из сомножителей, скажем, $h_i(\alpha)$, тоже лежит в P_1. Но тогда $\alpha \in h_i^{-1}(P_1)$, что противоречит выбору $\alpha \equiv 1 \pmod{P_1 \dots P_g}$. Это противоречие завершает доказательство Предложения. $\square$

Следствие. Если $F : \mathbb{Q}$ — расширение Галуа степени n, то $(p) = P_1^e \dots P_g^e$, все степени $f_{P_1} = \ldots = f_{P_g}$ равны f, и $efg = n$.

Доказательство: Все сомножители переставляются группой Галуа, следовательно степени $\deg P_i$ все равны между собой. Обозначим их общее значение через f. Пусть P^i входит в разложение (p) в степени e_i, а P_j — в степени e_j. Так как некоторый элемент $h \in \mathrm{Gal}(F : \mathbb{Q})$ переводит P_i в P_j, но сохраняет разложение (p) (ввиду его единственности), мы заключаем, что $e_i = e_j$, то есть все показатели равны между собой. Их общее значение обозначается e. Остается применить первую Теорему. $\square$

Часть 28. Поведение идеалов в квадратичных полях.

Пусть $d \in \mathbb{Z}$ — число свободное от квадратов. Как мы знаем из задачи 1 к 4 ноября, кольцо целых $A \subset \mathbb{Q}(\sqrt{d})$ равняется $\mathbb{Z}[\sqrt{d}]$, если $d = 2, 3 \pmod 4$, и $\mathbb{Z} \oplus \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, если $d = 1 \pmod 4$. Дискриминант $D(A)$ равняется в этих случаях, соответственно, $4d$ или d. Единственный нетривиальный элемент группы Галуа $\mathrm{Gal}(\mathbb{Q}(\sqrt{d}) : \mathbb{Q})$ будем обозначать $x \mapsto \overline{x}$. Опишем закон разложения нечетных простых чисел в нашем квадратичном расширении. Пусть $p \in \mathbb{Z}$ — нечетное простое число, и $P \subset A$ — простой идеал, делящий (p).

Теорема. a) Пусть p не делит $D(A)$ и уравнение $x^2 = d \pmod p$ неразрешимо в целых числах. Тогда $(p) = P,\ e_P = 1,\ f_P = 2$;

b) Пусть p не делит $D(A)$ и уравнение $x^2 = d \pmod p$ разрешимо в целых числах. Тогда $(p) = P\overline{P},\ P \neq \overline{P}, e_P = 1 = f_P$;

c) Если p делит $D(A)$, то $(p) = P^2,\ e_P = 2,\ f_P = 1$.

Вообще, если в разложении в произвольном поле Галуа $(p) = P_1^e \dots P_g^e$ имеет место один из крайних случаев $f = n,\ e = g = 1;\ g = n,\ f = e = 1;\ e = n,\ f = g = 1$, то говорят, соответственно, что *p остается инертным (вполне распадается, вполне ветвится) в F*. Таким образом, три случая нашей Теоремы служат иллюстрацией этих понятий. Кроме того, наша Теорема иллюстрирует тот факт, что в произвольном числовом поле F ветвятся те и только те простые p, которые делят дискриминант $D(F)$ (ср. также задачу 5 к 18 ноября). В частности, ветвится лишь конечное множество простых чисел. Геометрический аналог этого факта опять-таки очевиден (разветвленное накрытие $\mathbb{A}^1 \to \mathbb{A}^1, z \mapsto Q(z)$, ветвится лишь в конечном множестве точек комплексной прямой, а именно, в корнях дискриминанта многочлена $Q(z)$).

Доказательство: a) Так как $efg = 2$, достаточно проверить, что $f_P = 2 \;\Leftrightarrow\; A/P = \mathbb{F}_{p^2}$. Это означает, что не все классы вычетов $(\mathrm{mod}\ P)$ реализуются обычными целыми числами, т.е. $\mathbb{Z}/p\mathbb{Z} \subsetneqq A/P$. Но наше условие как раз и состоит в том, что класс $\sqrt{d} \pmod P$ не реализуется никаким обычным целым числом x. $\square$

b) Пусть $a \in \mathbb{Z}$ — решение уравнения $a^2 = d \pmod p$, т.е. $a^2 - d$ делится на p. Докажем, что $(p) = (p, a+\sqrt{d})(p, a-\sqrt{d})$. В самом деле, $(p, a + \sqrt{d})(p, a - \sqrt{d}) = (p^2, p(a + \sqrt{d}), p(a - \sqrt{d}), a^2 - d) = (p)(p, a + \sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p}) = (p)$, так как идеал $(p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p})$ содержит взаимно простые числа p и $2a$, т.е. совпадает со всем кольцом A. Осталось проверить, что $(p, a + \sqrt{d}) \neq (p, a - \sqrt{d})$. Иначе бы оба эти идеала содержали p и $2a$ и равнялись A. $\square$

c) $(p, \sqrt{d})^2 = (p^2, p\sqrt{d}, d) = (p)(p, \sqrt{d}, \frac{d}{p}) = (p)$, так как идеал $(p, \sqrt{d}, \frac{d}{p})$ содержит взаимно простые числа p и d (напомним, что d свободно от квадратов), т.е. совпадает со всем кольцом A. $\square$

Для сокращения формулировки Теоремы удобно воспользоваться *символом Лежандра*: в случае a) говорят, что $(\frac{d}{p}) = -1$; в случае b) говорят, что $(\frac{d}{p}) = 1$; в случае c) говорят, что $(\frac{d}{p}) = 0$.

Часть 29. Круговые поля.

Пусть $l \in \mathbb{Z}$ — нечетное простое число. Пусть $\zeta \in \mathbb{C}$ — примитивный корень l-ой степени из 1. Напомним, что минимальным многочленом z является многочлен $x^{l-1} + \ldots + x^2 + x + 1$. Его поле разложения — круговое поле $\mathbb{Q}(\zeta)$ имеет степень $l-1$ над $\mathbb{Q}$. Это расширение Галуа с группой Галуа $\mathbb{F}_l^*$.

Теорема. Кольцо целых $A \subset \mathbb{Q}(\zeta)$ равняется $\mathbb{Z}[\zeta]$.

Во всяком случае, очевидно, ζ является целым алгебраическим числом, а потому $A \supset \mathbb{Z}[\zeta]$. Докажем сначала следующую лемму.

Лемма. $(l) = (1-\zeta)^{l-1}$ (равенство идеалов в A).

Доказательство: Подставляя в наш минимальный многочлен 1, убеждаемся, что $l = \prod_{i=1}^{l-1}(1-\zeta^i)$. Заметим, что $u_i := \frac{1-\zeta^i}{1-\zeta} = 1 + \zeta + \ldots + \zeta^{i-1} \in \mathbb{Z}[\zeta]$. Но $u_i^{-1} = \frac{1-\zeta}{1-\zeta^i}$ также лежит в $\mathbb{Z}[\zeta]$, так как ζ^i — тоже примитивный $\sqrt[l]{1}$, и можно поменять роли ζ^i и ζ. Значит, u_i — обратимый элемент кольца A, или как еще говорят, *единица*. Произведение $\prod_{i=1}^{l-1} u_i$ тоже является единицей. Но $l = (1-\zeta)^{l-1}\prod_{i=1}^{l-1} u_i$. $\square$

Доказательство Теоремы: Как мы знаем, $1, \zeta, \ldots, \zeta^{l-2}$ образуют базис $\mathbb{Q}(\zeta)$ над $\mathbb{Q}$. Мы хотим доказать, что они образуют базис A над $\mathbb{Z}$. Возьмем $\alpha \in A$ и запишем $\alpha = a_0 + \ldots + a_{l-2}\zeta^{l-2}$, $a_i \in \mathbb{Q}$. Мы хотим доказать, что $a_i \in \mathbb{Z}$. Перво-наперво докажем, что $la_i \in \mathbb{Z}$. Для краткости будем обозначать $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ через Tr. Тогда $Tr(1) = l-1$, $Tr(\zeta^i) = -1$, откуда $Tr(\alpha\zeta) = -\sum_{i=0}^{l-2} a_i$, а при $0 \leqslant s \leqslant l-2$ имеем $Tr(\alpha\zeta^{-s}) = -\sum_{i=0}^{l-2} a_i + la_s$. Отсюда $Tr(\alpha\zeta^{-s} - \alpha\zeta) = la_s$. Так как $\alpha\zeta^{-s} - \alpha\zeta \in A$, левая часть является целым числом (т.е. лежит в $\mathbb{Z}$). Значит, и правая тоже.

Итак, мы можем записать $l\alpha = b_0 + b_1\zeta + \ldots + b_{l-2}\zeta^{l-2}$, $b_i \in \mathbb{Z}$. Обозначим $(1-\zeta)$ через η. Тогда можно заменить переменную в предыдущем равенстве: $l\alpha = c_0 + c_1\eta + \ldots + c_{l-2}\eta^{l-2}$, $c_i \in \mathbb{Z}$. Из Леммы мы знаем, что l делится на η. Следовательно, $l\alpha$ делится на η, откуда c_0 делится на η. Будучи целым числом, c_0 с необходимостью делится и на l: $c_0 = lc_0'$. Из Леммы мы знаем, что l делится на η^2. Отсюда выводим, что c_1 делится на η, а стало быть и на l: $c_1 = lc_1'$. Продолжая в том же духе, убеждаемся, что все c_i делятся на l, откуда все b_i делятся на l, откуда все a_i целые. $\square$

Лемма. Пусть $p \in \mathbb{Z}$ — простое число, $p \neq l$. Для некоторого n имеем $p^n = 1 \pmod{l}$. Тогда для всех $\alpha \in A$ имеем $\alpha^{p^n} = \alpha \pmod{p}$.

Доказательство: Запишем α в виде $\alpha = \sum_{i=0}^{l-2} a_i\zeta^i$. Тогда по малой теореме Ферма $\alpha^p \equiv \sum_i a_i^p\zeta^{pi} \pmod{p} \equiv \sum_i a_i\zeta^{pi} \pmod{p}$. Возведем в p-ую степень n раз и получим $\alpha^{p^n} \equiv \sum_i a_i\zeta^{p^n i} \pmod{p} = \sum_i a_i\zeta^i = \alpha$. $\square$

Следствие. $p \neq l$ неразветвлено в $\mathbb{Q}(\zeta)$.

Доказательство: Иначе бы $(p) \subset P^2$ для какого-то простого идеала $P \subset A$. Имеем $P \supset P^2 \supset (p)$, а значит, можно выбрать $\alpha \in P$, $\alpha \notin P^2$. По Лемме $\alpha^{p^n} \equiv \alpha \pmod p$, откуда $\alpha^{p^n} \equiv \alpha \pmod P)^2$. Но $p^n > 1$, следовательно, $\alpha^{p^n} \in P^2 \Rightarrow \alpha \in P^2$ — противоречие. $\square$

Это следствие вместе с задачей 2 к 25 ноября опять подтверждает тот факт, что ветвятся только делители дискриминанта.

Часть 30. Квадратичный закон взаимности Гаусса.

Поскольку $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) = \mathbb{F}_l^*$, имеется естественное отображение из $\mathbb{Z} - l\mathbb{Z}$ в $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$. Образ простого числа $p \in \mathbb{Z} - l\mathbb{Z}$ при этом отображении будем называть *p-ый Фробениус* и обозначать $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$. Тогда $\sigma_p(\zeta) = \zeta^p$.

Предложение. Пусть $\alpha \in A$. Тогда $\sigma_p(\alpha) \equiv \alpha^p \pmod p$.

Доказательство: Запишем α в виде $\alpha = \sum_i a_i\zeta^i$. Тогда $\sigma_p(\alpha) = \sum_i a_i\zeta^{pi} \equiv \sum_i a_i^p\zeta^{pi} \pmod p \equiv \alpha^p \pmod p$, как мы видели при доказательстве предыдущей Леммы. $\square$

Положим $l' = (-1)^{\frac{l-1}{2}}l$. По задаче 6 к 30 сентября, $\sqrt{l'}$ лежит в $\mathbb{Q}(\zeta)$. В самом деле, $l = \prod_{i=1}^{l-1}(1-\zeta^i) = \prod_{i=1}^{\frac{l-1}{2}}(1-\zeta^i)(1-\zeta^{-i}) = \prod_{i=1}^{\frac{l-1}{2}}(1-\zeta^i)^2(-\zeta^{-i})\prod_{i=1}^{\frac{l-1}{2}}(1-\zeta^i)^2(-1)^{\frac{l-1}{2}}\zeta^{-1-2-\ldots-\frac{l-1}{2}} = \prod_{i=1}^{\frac{l-1}{2}}(1-\zeta^i)^2(-1)^{\frac{l-1}{2}}\zeta^{-\frac{l^2-1}{8}}$. Возьмем $m \in \mathbb{Z}$ так, чтобы $2m \equiv \frac{l^2-1}{8} \pmod l$. Тогда последнее равенство переписывается в виде $l' = \left(\zeta^{-m}\prod_{i=1}^{\frac{l-1}{2}}(1-\zeta^i)\right)^2$. Обозначим $\sqrt{l'} = \zeta^{-m}\prod_{i=1}^{\frac{l-1}{2}}(1-\zeta^i)$ через $\lambda \in A$.

Рассмотрим башню полей $\mathbb{Q}(\zeta) \supset \mathbb{Q}(\lambda) \supset \mathbb{Q}$. Всякий элемент σ группы Галуа $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ действует на нормальном подполе $\mathbb{Q}(\lambda)$, $\sigma(\lambda) = \pm\lambda$. При этом знак $+$ имеет место тогда и только тогда, когда σ является квадратом в циклической группе $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) = \mathbb{F}_l^*$. Пользуясь обозначениями Лежандра, можно записать $\sigma(\lambda) = (\frac{\sigma}{l})\lambda$.

Пусть $p \in \mathbb{Z}$ — нечетное простое число, $p \neq l$. *Квадратичный закон взаимности Гаусса* гласит, что $(\frac{p}{l})(\frac{l}{p}) = (-1)^{\frac{p-1}{2}\frac{l-1}{2}}$. Символ Лежандра, очевидно, мультипликативен: $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$. Кроме того, как нам известно из первой лекции, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. Поэтому закон взаимности Гаусса можно переписать в следующей эквивалентной форме: $(\frac{l'}{p}) = (\frac{p}{l})$. Докажем его в таком виде.

Заметим, что $(l')^{p-1} \equiv 1 \pmod p$, а $(l')^{\frac{p-1}{2}} \equiv (\frac{l'}{p}) \pmod p$, так как мультипликативная группа остатков по модулю p циклична. Поэтому $\lambda^p = \lambda^{p-1}\lambda = (l')^{\frac{p-1}{2}}\lambda \equiv (\frac{l'}{p})\lambda \pmod p$. Итак, имеем цепочку равенств (второе равенство — это предыдущее Предложение): $(\frac{p}{l})\lambda = \sigma_p(\lambda) \equiv \lambda^p \pmod p \equiv (\frac{l'}{p})\lambda \pmod p$. Так как число p нечетно, выводим отсюда $(\frac{p}{l}) = (\frac{l'}{p})$. $\square$

Для полноты сообщим, что $(\frac{2}{p}) = 1$, если $p = \pm 1 \pmod 8$, и $(\frac{2}{p}) = -1$, если $p = \pm 3 \pmod 8$. Докажите это сами.

Удачи на зачете и экзамене! До следующего года!