5.3. Квадратичные поля и их кольца целых

1. Квадратичные расширения над $\mathbb{Q}$

Определение 0.1. Пусть $F/\mathbb{Q}$ — конечное расширение полей. Его *степенью* называется число

$$[F : \mathbb{Q}] = \dim_{\mathbb{Q}} F.$$

Определение 0.2. Поле F называется *квадратичным* над $\mathbb{Q}$, если $[F : \mathbb{Q}] = 2$.

Утверждение 0.3. *Если $F/\mathbb{Q}$ квадратично, то существует элемент $\alpha \in F\backslash\mathbb{Q}$ такой, что*

$$F = \mathbb{Q}(\alpha),$$

и минимальный многочлен α над $\mathbb{Q}$ имеет степень 2.

Утверждение 0.4. *Пусть $d \in \mathbb{Z}$ не является квадратом в $\mathbb{Z}$. Тогда*

$$F = \mathbb{Q}(\sqrt{d})$$

является квадратичным полем и

$$[F : \mathbb{Q}] = 2, \qquad \{1, \sqrt{d}\} \text{ — базис } F \text{ над } \mathbb{Q}.$$

Замечание 0.5. Обычно выбирают d *квадратсвободным* (squarefree), чтобы представление $\mathbb{Q}(\sqrt{d})$ было “нормальным”.

2. Группа Галуа квадратичного поля, след и норма

Рассмотрим квадратичное поле $F = \mathbb{Q}(\sqrt{d})$, где $d \in \mathbb{Z}$ не квадрат.

Утверждение 0.6.

$$\mathrm{Gal}(F/\mathbb{Q}) = \{\mathrm{id}, \sigma\}, \qquad \sigma(\sqrt{d}) = -\sqrt{d}.$$

Доказательство. Пусть $\tau \in \mathrm{Gal}(F/\mathbb{Q})$. Тогда τ фиксирует $\mathbb{Q}$ и переводит корни минимального многочлена $x^2 - d$ в корни того же многочлена. Следовательно,

$$\tau(\sqrt{d}) \in \{\sqrt{d}, -\sqrt{d}\}.$$

Это даёт ровно два автоморфизма: тождественный и сопряжение σ. □

Определение 0.7. Для $\alpha \in F$ определим *сопряжение* $\alpha' = \sigma(\alpha)$, а также *след* и *норму*:

$$\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = \alpha + \alpha', \qquad \mathrm{N}_{F/\mathbb{Q}}(\alpha) = \alpha\alpha'.$$

Если $\alpha = r + s\sqrt{d}$ (где $r, s \in \mathbb{Q}$), то

$$\alpha' = r - s\sqrt{d}, \qquad \mathrm{Tr}(\alpha) = 2r, \qquad \mathrm{N}(\alpha) = r^2 - ds^2.$$

3. Кольцо целых элементов квадратичного поля

Определение 0.8. Элемент $\alpha \in F$ называется *целым (алгебраически целым)* над $\mathbb{Z}$, если он является корнем некоторого унитарного многочлена $f(x) \in \mathbb{Z}[x]$. Множество всех целых элементов поля F обозначается $\mathcal{O}_F$ и называется *кольцом целых* поля F.

Лемма 0.9. *Пусть $F = \mathbb{Q}(\sqrt{d})$ и $\alpha \in F$. Тогда $\alpha \in \mathcal{O}_F$ тогда и только тогда, когда*

$$\mathrm{Tr}(\alpha) \in \mathbb{Z} \quad \text{и} \quad \mathrm{N}(\alpha) \in \mathbb{Z}.$$

Доказательство. ($\Rightarrow$) Если α целый, то он удовлетворяет унитарному многочлену степени 2:

$$x^2 - \mathrm{Tr}(\alpha)x + \mathrm{N}(\alpha) = 0,$$

причём коэффициенты этого многочлена лежат в $\mathbb{Z}$. Значит $\mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in \mathbb{Z}$.

($\Leftarrow$) Пусть $\mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in \mathbb{Z}$. Тогда α является корнем многочлена

$$x^2 - \mathrm{Tr}(\alpha)x + \mathrm{N}(\alpha) \in \mathbb{Z}[x],$$

который унитарен, значит α целый. $\square$

Теорема 0.10 (описание $\mathcal{O}_F$)**.** *Пусть $F = \mathbb{Q}(\sqrt{d})$, где d квадратсвободно. Тогда*

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod 4. \end{cases}$$

Доказательство. Пусть $\alpha = r + s\sqrt{d} \in F$ с $r, s \in \mathbb{Q}$. По лемме 0.9 нужно и достаточно:

$$\mathrm{Tr}(\alpha) = 2r \in \mathbb{Z}, \qquad \mathrm{N}(\alpha) = r^2 - ds^2 \in \mathbb{Z}.$$

Из $2r \in \mathbb{Z}$ получаем $r = \dfrac{m}{2}$ для некоторого $m \in \mathbb{Z}$.

Пусть также $s = \dfrac{n}{2}$ для некоторого $n \in \mathbb{Z}$ (это будет следовать из условия на норму). Тогда

$$\mathrm{N}(\alpha) = \left(\frac{m}{2}\right)^2 - d\left(\frac{n}{2}\right)^2 = \frac{m^2 - dn^2}{4} \in \mathbb{Z},$$

то есть

$$m^2 - dn^2 \equiv 0 \pmod 4.$$

Рассмотрим случаи по $d \bmod 4$.

Случай 1: $d \equiv 2, 3 \pmod 4$**.** Если n нечётно, то $n^2 \equiv 1 \pmod 4$, и тогда

$$m^2 - dn^2 \equiv m^2 - d \pmod 4.$$

Но при $d \equiv 2, 3 \pmod 4$ число d не сравнимо с квадратом по модулю 4 так, чтобы получилось 0 для любого m, откуда следует, что n должен быть чётным, то есть $s \in \mathbb{Z}$. Тогда и $r \in \mathbb{Z}$ (иначе нарушится целочисленность нормы). Значит $\alpha \in \mathbb{Z}[\sqrt{d}]$, и получаем $\mathcal{O}_F = \mathbb{Z}[\sqrt{d}]$.

Случай 2: $d \equiv 1 \pmod 4$**.** Тогда условие $m^2 - dn^2 \equiv 0 \pmod 4$ эквивалентно

$$m^2 - n^2 \equiv 0 \pmod 4 \quad \Longleftrightarrow \quad m \equiv n \pmod 2.$$

Следовательно,

$$\alpha = \frac{m+n\sqrt{d}}{2}, \qquad m \equiv n \pmod 2.$$

Положим $\omega = \dfrac{1+\sqrt{d}}{2}$. Тогда любой такой α можно записать как

$$\alpha = a + b\omega, \qquad a, b \in \mathbb{Z},$$

и наоборот, каждый $a + b\omega$ целый. Значит $\mathcal{O}_F = \mathbb{Z}[\omega]$. $\square$

4. Дискриминант квадратичного поля

Определение 0.11. Пусть $F/\mathbb{Q}$ — расширение степени n, и $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_F$. Определим *дискриминант* набора $(\alpha_1, \ldots, \alpha_n)$:

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det\bigl(\mathrm{Tr}(\alpha_i \alpha_j)\bigr)_{i,j=1}^{n}.$$

Дискриминант поля (точнее, дискриминант кольца целых) обозначают $\mathrm{disc}(F)$.

Утверждение 0.12. *Пусть $F = \mathbb{Q}(\sqrt{d})$, d квадратсвободно. Тогда*

$$\mathrm{disc}(F) = \begin{cases} 4d, & d \equiv 2, 3 \pmod 4, \\ d, & d \equiv 1 \pmod 4. \end{cases}$$

Доказательство. Если $d \equiv 2, 3 \pmod 4$, то базис $\mathcal{O}_F$ равен $(1, \sqrt{d})$. Считаем матрицу следов:

$$\mathrm{Tr}(1 \cdot 1) = 2, \quad \mathrm{Tr}(1 \cdot \sqrt{d}) = \mathrm{Tr}(\sqrt{d}) = 0, \quad \mathrm{Tr}(\sqrt{d} \cdot \sqrt{d}) = \mathrm{Tr}(d) = 2d.$$

Значит

$$\Delta(1, \sqrt{d}) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Если $d \equiv 1 \pmod 4$, то базис $\mathcal{O}_F$ равен $(1, \omega)$, где $\omega = \dfrac{1+\sqrt{d}}{2}$. Тогда $\omega' = \dfrac{1-\sqrt{d}}{2}$, и

$$\mathrm{Tr}(1) = 2, \qquad \mathrm{Tr}(\omega) = \omega + \omega' = 1, \qquad \mathrm{Tr}(\omega^2) = \omega^2 + (\omega')^2.$$

Заметим:

$$\omega^2 = \frac{(1+\sqrt{d})^2}{4} = \frac{1+2\sqrt{d}+d}{4}, \qquad (\omega')^2 = \frac{1-2\sqrt{d}+d}{4},$$

поэтому

$$\mathrm{Tr}(\omega^2) = \frac{1+d}{2}.$$

Следовательно,

$$\Delta(1, \omega) = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = 2 \cdot \frac{1+d}{2} - 1 = d.$$

$\square$

5. Разложение простого идеала (p) в $\mathcal{O}_F$

Пусть $F = \mathbb{Q}(\sqrt{d})$, d квадратсвободно, $\mathcal{O}_F$ — кольцо целых.

Теорема 0.13 (квадратичный закон разложения простого)**.** *Пусть p — нечётное простое, $p \nmid \operatorname{disc}(F)$. Тогда в $\mathcal{O}_F$ возможны ровно три случая:*

1. ***Расщепление:*** *если $\left(\frac{d}{p}\right) = 1$, то*
$$(p) = \mathfrak{p}\,\mathfrak{p}', \qquad \mathfrak{p} \neq \mathfrak{p}', \qquad \mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{p}') = p.$$
2. ***Инертность:*** *если $\left(\frac{d}{p}\right) = -1$, то (p) прост в $\mathcal{O}_F$ и*
$$(p) \text{ остаётся простым}, \qquad \mathrm{N}((p)) = p^2.$$
3. ***Разветвление:*** *если $p \mid \operatorname{disc}(F)$, то*
$$(p) = \mathfrak{p}^2, \qquad \mathrm{N}(\mathfrak{p}) = p.$$

Замечание 0.14. Случай $p \mid \operatorname{disc}(F)$ — это именно *разветвление*. Для нечётного p это эквивалентно $p \mid d$.

6. Частный разбор: конструкция идеалов при $\left(\frac{d}{p}\right) = 1$

Пусть p — нечётное простое, $p \nmid d$ и $\left(\frac{d}{p}\right) = 1$. Тогда существует $a \in \mathbb{Z}$ такое, что
$$a^2 \equiv d \pmod{p}.$$

Рассмотрим идеалы
$$\mathfrak{p} = (p,\, a + \sqrt{d}), \qquad \mathfrak{p}' = (p,\, a - \sqrt{d}).$$

Утверждение 0.15. *Имеем включение*
$$\mathfrak{p}\mathfrak{p}' \subseteq (p).$$

Доказательство. Действительно, в произведении $\mathfrak{p}\mathfrak{p}'$ лежат элементы вида
$$p \cdot p, \quad p(a - \sqrt{d}), \quad p(a + \sqrt{d}), \quad (a + \sqrt{d})(a - \sqrt{d}) = a^2 - d.$$

Первые три очевидно кратны p, а для последнего имеем $a^2 - d \equiv 0 \pmod{p}$, значит $a^2 - d \in (p)$. ☐

Утверждение 0.16. *Идеалы $\mathfrak{p} \neq \mathfrak{p}'$ и*
$$(p) = \mathfrak{p}\mathfrak{p}'.$$

Замечание 0.17. На картинке у преподавателя это записано как “строим два разных простых идеала над p”.

7. Замечания про $p = 2$

Для $p = 2$ разложение зависит от $d \bmod 8$ и вида $\mathcal{O}_F$. Обычно отдельно разбирают случаи $d \equiv 1 \pmod 8$, $d \equiv 5 \pmod 8$ и т.д., потому что дискриминант может содержать степень двойки.

Итого по страницам:

- определили квадратичное поле $F = \mathbb{Q}(\sqrt{d})$;
- описали $\mathrm{Gal}(F/\mathbb{Q})$ и сопряжение;
- ввели Tr и N;
- через Tr, N описали $\mathcal{O}_F$;
- вычислили $\mathrm{disc}(F)$;
- сформулировали правило разложения (p) по символу Лежандра $\left(\frac{d}{p}\right)$;
- показали конструкцию идеалов $\mathfrak{p} = (p, a + \sqrt{d})$ при $\left(\frac{d}{p}\right) = 1$.

Разложение простого идеала (p) в квадратичном поле

Пусть $F = \mathbb{Q}(\sqrt{d})$, d — квадратсвободное целое, $D = \mathcal{O}_F$. Для $\alpha = r + s\sqrt{d} \in F$ (где $r, s \in \mathbb{Q}$) обозначим сопряжение

$$\alpha' = r - s\sqrt{d}.$$

Для идеала $P \subset D$ положим

$$P' = \{\gamma' \mid \gamma \in P\}.$$

Тогда P' тоже идеал в D (сопряжённый к P).

Напоминание про типы разложения. Пусть

$$(p) = P_1^{e_1} \cdots P_g^{e_g}, \qquad N(P_i) = p^{f_i}.$$

Тогда выполняется равенство $\sum_{i=1}^{g} e_i f_i = [F : \mathbb{Q}] = 2$. Отсюда возможны ровно три случая:

(a) разветвление: $(p) = P^2, \quad e = 2,\ f = 1,\ g = 1;$
(b) разложение: $(p) = PP', \quad e = 1,\ f = 1,\ g = 2,\ P \neq P';$
(c) инертность: $(p) = P, \quad e = 1,\ f = 2,\ g = 1.$

Теорема 0.18 (Критерий разложения через дискриминант). *Пусть p — нечётное простое, $p \neq 2$. Тогда:*

$$\left(\frac{\delta_F}{p}\right) = \begin{cases} 0 & \iff p \mid \delta_F \implies (p) = P^2, \\ 1 & \iff p \nmid \delta_F \implies (p) = PP',\ P \neq P', \\ -1 & \iff p \nmid \delta_F \implies (p) \text{ прост в } D. \end{cases}$$

Случай 1: $\left(\frac{\delta_F}{p}\right) = 0$ (разветвление)

Предположим $p \mid \delta_F$. Для квадратичного поля $F = \mathbb{Q}(\sqrt{d})$ имеем $\delta_F \in \{d,\, 4d\}$, поэтому из $p \mid \delta_F$ следует $p \mid d$.

Положим

$$P = (p, \sqrt{d}) = \{\alpha p + \beta\sqrt{d} \mid \alpha, \beta \in D\}.$$

Тогда

$$P^2 = (p, \sqrt{d})^2 = (p^2,\ p\sqrt{d},\ d).$$

Так как $p \mid d$, то $d = p \cdot \frac{d}{p}$ и

$$(p^2,\ p\sqrt{d},\ d) \subset (p) \cdot (p, \sqrt{d}, d/p).$$

Обозначим

$$I = (p, \sqrt{d}, d/p).$$

Поскольку $p \mid d$, число $d/p \in \mathbb{Z} \subset D$. Кроме того,

$$(p,\ d/p) = 1 \quad \Rightarrow \quad \exists\, r, s \in \mathbb{Z} :\ rp + s\frac{d}{p} = 1,$$

значит $1 \in I$, то есть $I = D$. Следовательно,

$$P^2 \subset (p) \cdot I = (p).$$

С другой стороны, очевидно $(p) \subset P$, значит $(p)^2 \subset P^2$, а так как индекс $[D : P] = p$, то $(p) \neq P$ и единственная возможность при степени 2:

$$(p) = P^2.$$

Случай 2: $\left(\frac{\delta_F}{p}\right) = 1$ (разложение)

Пусть $\left(\frac{\delta_F}{p}\right) = 1$. Тогда $p \nmid \delta_F$ и (для нечётного p) это эквивалентно $\left(\frac{d}{p}\right) = 1$, то есть существует $a \in \mathbb{Z}$ такое, что

$$a^2 \equiv d \pmod{p}.$$

Определим идеалы

$$P = (p,\ a + \sqrt{d}), \qquad P' = (p,\ a - \sqrt{d}).$$

Тогда

$$PP' \subset (p,\ a + \sqrt{d})(p,\ a - \sqrt{d}) \subset (p,\ a + \sqrt{d},\ a - \sqrt{d},\ \tfrac{a^2 - d}{p}).$$

Обозначим

$$I = (p,\ a + \sqrt{d},\ a - \sqrt{d},\ \tfrac{a^2 - d}{p}).$$

Заметим, что

$$2a = (a + \sqrt{d}) + (a - \sqrt{d}) \in I, \qquad 2\sqrt{d} = (a + \sqrt{d}) - (a - \sqrt{d}) \in I.$$

Кроме того, по построению $\frac{a^2 - d}{p} \in \mathbb{Z} \subset D$, поэтому

$$(p,\ 2a,\ \tfrac{a^2 - d}{p}) = 1 \ \Rightarrow\ 1 \in I \ \Rightarrow\ I = D.$$

Следовательно,
$$PP' \subset (p) \cdot I = (p).$$
Обратно, поскольку $p \in P$ и $p \in P'$, имеем $(p) \subset PP'$. Итак,
$$(p) = PP'.$$
Покажем, что $P \neq P'$. Если бы $P = P'$, то из $a + \sqrt{d} \in P = (p, a - \sqrt{d})$ следовало бы
$$(a + \sqrt{d}) - (a - \sqrt{d}) = 2\sqrt{d} \in P.$$
Тогда $\sqrt{d} \in P$ (так как p нечётное, 2 обратимо по модулю P), а значит $P \supset (p, \sqrt{d})$, что в сочетании с $p \nmid d$ приводит к противоречию (в этом случае $(p, \sqrt{d}) = D$). Следовательно, $P \neq P'$.

Случай 3: $\left(\frac{\delta_F}{p}\right) = -1$ (инертность)

Пусть $\left(\frac{\delta_F}{p}\right) = -1$, то есть $p \nmid \delta_F$ и $\left(\frac{d}{p}\right) = -1$.

Предположим противное: (p) не прост в D. Тогда
$$(p) = PP'$$
для некоторых различных простых идеалов $P \neq P'$ и при этом обязательно $f = 1$, то есть
$$|D/P| = p.$$
Рассмотрим класс $\overline{\sqrt{d}} \in D/P$. Так как $D/P \simeq \mathbb{F}_p$, существует $a \in \mathbb{Z}$ такое, что $\overline{\sqrt{d}} = \overline{a}$ в D/P, то есть
$$\sqrt{d} - a \in P \quad \Rightarrow \quad d - a^2 \in P \cap \mathbb{Z} = (p).$$
Значит $a^2 \equiv d \pmod{p}$, то есть $\left(\frac{d}{p}\right) = 1$ — противоречие. Следовательно, разложения нет и остаётся единственный вариант:
$$(p) \text{ прост в } D, \qquad f = 2.$$

Замечание про случай $p = 2$

Далее рассматривается $p = 2$ отдельно. Возможны три ситуации:

$$\begin{array}{ll} \text{(i)} & 2 \mid \delta_F \implies (2) = P^2; \\ \text{(ii)} & 2 \nmid \delta_F,\ d \equiv 1 \pmod{8} \implies (2) = PP',\ P \neq P'; \\ \text{(iii)} & 2 \nmid \delta_F,\ d \equiv 5 \pmod{8} \implies (2) \text{ прост в } D. \end{array}$$

Критерий единицы (пометка на полях)

Для $\alpha \in D$:
$$\alpha \in D^\times \iff N_{F/\mathbb{Q}}(\alpha) = \pm 1.$$

Случай $d < 0$

Пусть $d < 0$. Обозначим через $\mathcal{D}$ кольцо целых поля $\mathbb{Q}(\sqrt{d})$. Тогда группа единиц

$$U_d = \mathcal{D}^{\times}$$

конечна.

1. При $d = -1$:
$$U_{-1} = \{\pm 1, \pm i\}, \qquad |U_{-1}| = 4.$$
2. При $d = -3$:
$$U_{-3} = \{\pm 1, \pm \omega, \pm \omega^2\}, \qquad \omega = \frac{-1 + \sqrt{-3}}{2}, \qquad |U_{-3}| = 6.$$
3. При $d < -3$:
$$U_d = \{\pm 1\}.$$

Доказательство. Пусть $x + y\sqrt{d} \in \mathcal{D}$ — единица. Тогда

$$x^2 - dy^2 = \pm 1.$$

Если $|d| > 1$, то при $y \neq 0$ имеем

$$x^2 + |d|y^2 \geq |d| > 1,$$

что невозможно. Следовательно, $y = 0$, откуда $x = \pm 1$. $\square$

Циклотомические поля

Пусть $m \geq 1$,

$$\zeta_m = e^{2\pi i/m}, \qquad F = \mathbb{Q}(\zeta_m).$$

Тогда

$$x^m - 1 = \prod_{d \mid m} \Phi_d(x),$$

где $\Phi_m(x)$ — m-й циклотомический многочлен.

$$\deg \Phi_m = \varphi(m).$$

Следовательно,

$$[F : \mathbb{Q}] = \varphi(m).$$

Группа Галуа циклотомического поля

Рассмотрим

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}).$$

Для $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ имеем

$$\sigma(\zeta_m)^m = 1,$$

то есть

$$\sigma(\zeta_m) = \zeta_m^a, \qquad (a, m) = 1.$$

Тем самым получаем отображение

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^{\times}, \qquad \sigma \mapsto a.$$

Лемма 0.19. *Это отображение является изоморфизмом групп.*

Доказательство. Инъективность следует из того, что автоморфизм однозначно задаётся образом ζ_m. Сюръективность следует из того, что для каждого $(a, m) = 1$ отображение

$$\zeta_m \mapsto \zeta_m^a$$

задаёт автоморфизм поля. □

Следовательно,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times.$$

Композиция автоморфизмов

Пусть $\sigma_a, \sigma_b \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, где

$$\sigma_a(\zeta_m) = \zeta_m^a, \qquad \sigma_b(\zeta_m) = \zeta_m^b.$$

Тогда

$$\sigma_a \circ \sigma_b(\zeta_m) = \sigma_a(\zeta_m^b) = \zeta_m^{ab}.$$

Отсюда

$$\sigma_a \circ \sigma_b = \sigma_{ab}.$$

Нейтральный элемент:

$$\sigma_1 = \mathrm{id}.$$

Обратный элемент:

$$\sigma_a^{-1} = \sigma_{a^{-1}}, \qquad aa^{-1} \equiv 1 \pmod{m}.$$

Тем самым группа автоморфизмов изоморфна

$$(\mathbb{Z}/m\mathbb{Z})^\times.$$

Циклотомические поля

Пусть $m \geq 1$ и

$$\zeta_m = e^{2\pi i/m}.$$

Определим циклотомическое поле

$$K = \mathbb{Q}(\zeta_m).$$

Теорема 0.20. *Поле $\mathbb{Q}(\zeta_m)$ является расширением Галуа над $\mathbb{Q}$, и*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times.$$

Доказательство. Каждому $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ сопоставим автоморфизм

$$\sigma_a(\zeta_m) = \zeta_m^a.$$

Так как $(a, m) = 1$, отображение корректно и сохраняет минимальный многочлен ζ_m. Композиция автоморфизмов соответствует умножению по модулю m, следовательно,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

□

Следствие 0.21.

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m).$$

Циклотомический многочлен

Определение 0.22. *Циклотомическим многочленом* $\Phi_m(x)$ называется минимальный многочлен числа ζ_m над $\mathbb{Q}$.

Из определения следует:

$$x^m - 1 = \prod_{d|m} \Phi_d(x).$$

Теорема 0.23. *Многочлен $\Phi_m(x)$ имеет целые коэффициенты и неприводим над $\mathbb{Q}$.*

Доказательство. Докажем индукцией по m. Предположим, что все $\Phi_d(x) \in \mathbb{Z}[x]$ для $d < m$. Тогда из разложения

$$\Phi_m(x) = \frac{x^m - 1}{\prod_{d|m,\, d<m} \Phi_d(x)}$$

следует, что $\Phi_m(x) \in \mathbb{Z}[x]$.

Неприводимость следует из того, что все сопряжения ζ_m^a, $(a, m) = 1$, являются корнями $\Phi_m(x)$, и их число равно $\varphi(m)$. □

Дискриминант циклотомического поля

Пусть $K = \mathbb{Q}(\zeta_m)$.

Теорема 0.24. *Дискриминант поля $\mathbb{Q}(\zeta_m)$ равен*

$$\mathrm{Disc}(K) = (-1)^{\varphi(m)/2} \frac{m^{\varphi(m)}}{\prod_{p|m} p^{\varphi(m)/(p-1)}}.$$

Доказательство. Используется формула дискриминанта через произведение разностей сопряжённых корней:

$$\Delta = \prod_{i<j} (\zeta_m^i - \zeta_m^j)^2.$$

После перегруппировки и применения свойств корней из единицы получается указанная формула. □

Разложение простых в циклотомических полях

Пусть p — простое число.

Теорема 0.25. *Если $p \nmid m$, то разложение идеала (p) в $\mathbb{Z}[\zeta_m]$ определяется порядком p по модулю m.*

Доказательство. Пусть f — наименьшее число, такое что

$$p^f \equiv 1 \pmod{m}.$$

Тогда минимальный многочлен ζ_m по модулю p распадается на $\varphi(m)/f$ неприводимых множителей степени f. Следовательно,

$$(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_{\varphi(m)/f}, \quad \deg \mathfrak{p}_i = f.$$

□

Следствие 0.26. *Простое p полностью раскладывается в $\mathbb{Q}(\zeta_m)$ тогда и только тогда, когда*

$$p \equiv 1 \pmod{m}.$$

Связь с кольцами вычетов

Теорема 0.27. *Существует изоморфизм*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathrm{Aut}(\mu_m) \cong (\mathbb{Z}/m\mathbb{Z})^\times,$$

где μ_m — группа корней m-й степени из единицы.

Заключение

Циклотомические поля являются фундаментальным примером абелевых расширений поля $\mathbb{Q}$. Они играют ключевую роль в:

- теории Галуа,
- разложении простых в числовых полях,
- доказательстве теоремы Кронекера–Вебера,
- арифметике круговых полей.