## 5.3 Квадратичные поля
## Квадратичные поля

$\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ $\qquad \mathbb{Z}[i] = \{a+bi,\ a,b \in \mathbb{Z}\}$

$\mathbb{Q}(i)$, $\mathbb{Q}(\omega)$

Опр: $F/\mathbb{Q}$, $[F:\mathbb{Q}] = 2$, $F$ — квадр.

$F = \mathbb{Q}(\alpha)$, $\alpha$ — корень $ax^2+bx+c \in \mathbb{Z}[x]$

$D = D_{\mathbb{Q}(\alpha)}$ — кольцо целых $\quad | \quad D_K = \{\alpha \in K : f(\alpha) = 0,\ f \in \mathbb{Z}[x]\}$

$$\alpha = \frac{-b \pm \sqrt{b^2-4ac}}{2a}, \qquad F = \mathbb{Q}(\sqrt{b^2-4ac})$$

$D = D_1^2 d$

($D = \mathbb{Z}[\alpha]$ ? — не всегда)

$F = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ / св. от кв.

$Gal(F/\mathbb{Q})$. $\quad ( \ |Gal(F/\mathbb{Q})| = [F : \mathbb{Q}] \ )$

$\sigma \in G = Gal(F/\mathbb{Q}) \qquad (\sqrt{d})^2 = d$

$(\sigma\sqrt{d})^2 = d \quad \Rightarrow \quad \sigma\sqrt{d} = \pm\sqrt{d}$

$\sigma\sqrt{d} = \sqrt{d}$ тожд. $\qquad \sigma\sqrt{d} = -\sqrt{d}$ $\quad$ (П: $a+ib \mapsto a-ib$)

$G = \{ id, \ \underbrace{\sqrt{d} \mapsto -\sqrt{d}}_{\sigma} \}$, $\quad F/\mathbb{Q}$ — расш. Галуа

$\alpha \in F \qquad \alpha = r + s\sqrt{d}, \quad r, s \in \mathbb{Q}$

$\sigma(\alpha) = r - s\sqrt{d} = \alpha'$ — сопр.

$Tr\,\alpha = \alpha + \alpha' = 2r \qquad N\alpha = \alpha\alpha' = r^2 - ds^2$

Лемма) $\gamma \in \mathcal{O} \Leftrightarrow Tr\,\gamma, \ N\gamma \in \mathbb{Z}$

$\square$ ... $\quad (x-\gamma)(x-\gamma') = x^2 - (\gamma+\gamma')x + \gamma\gamma'$ $\blacksquare$

Теорема: $\mathcal{D} = \mathcal{D}_{\mathbb{Q}(\sqrt{d})}$

$$\mathcal{D} = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2, 3\ (4) \\ \mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right], & d \equiv 1\ (4) \end{cases}$$

Д: $\gamma = r + s\sqrt{d} \in \mathcal{D} \Leftrightarrow 2r,\ r^2 - ds^2 \in \mathbb{Z}$

$r, s \in \mathbb{Q}$ $\qquad \Rightarrow 4ds^2 \in \mathbb{Z} \Rightarrow 2s \in \mathbb{Z}$

$m = 2r$, $n = 2s$, $m, n \in \mathbb{Z}$

$m^2 - dn^2 = 4(r^2 - s^2 d) \equiv 0\ (4)$.

$m^2, n^2 \equiv 0, 1\ (4)$, $d \equiv 1, 2, 3\ (4)$

Если

$d \equiv 2\ (4)$ $\qquad m^2 - dn^2 \equiv m^2 + 2n^2\ (4)$

$d \equiv 3\ (4)$ $\qquad m^2 - dn^2 \equiv m^2 + n^2\ (4)$

$\Rightarrow m \equiv n \equiv 0\ (2) \Rightarrow r, s \in \mathbb{Z} \Rightarrow \mathcal{D} = \mathbb{Z}[\sqrt{d}]$

$d \equiv 1 \ (4)$ $\quad m^2 - dn^2 \equiv m^2 - n^2 \ (4)$

$\Rightarrow$ или $m \equiv n \equiv 0 \ (2)$ или $m \equiv n \equiv 1 \ (2)$

$\Rightarrow \mathcal{O} = \{ \frac{1}{2} m + \frac{1}{2} n\sqrt{d} \ : \ m \equiv n \ (2) \}$

$$\frac{m+n}{2} + n\left(\frac{-1+\sqrt{d}}{2}\right) \Rightarrow \mathcal{O} \subset \underbrace{\mathbb{Z} + \mathbb{Z}\left(\frac{-1+\sqrt{d}}{2}\right)}_{\mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right]}$$

$$\frac{-1+\sqrt{d}}{2} \in \mathcal{O} \Rightarrow \mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right] \subset \mathcal{O} \quad \blacksquare$$

<u>Лемма</u>: $\delta_F$ — дискр. $F$, $\delta_F = \begin{cases} 4d, & d \equiv 2,3 \ (4) \\ d, & d \equiv 1 \ (4) \end{cases}$

(Опр: $L/K$, $\alpha_1, \dots, \alpha_n \in L$

$\Delta(\alpha_1, \dots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))$

$\alpha_i \in \mathcal{O}_K$ $\quad \Delta(\alpha_1, \dots, \alpha_n)$ не зав. от выбора базиса )

$\Delta = \delta_F$

$\square$ $\omega_1, \omega_2$ — баз. $D$ $\quad \delta_F = \det(\mathrm{Tr}(\omega_i \omega_j))$

$d \equiv 2, 3 \ (4)$ $\quad \omega_1 = 1, \ \omega_2 = \sqrt{d}$

$d \equiv 1 \ (4)$ $\quad \omega_1 = 1, \ \omega_2 = \dfrac{-1+\sqrt{d}}{2}$

2) ... $\blacksquare$

В простом поле: $[F:\mathbb{Q}] = n$

Теорема: $F:\mathbb{Q}$ — расш. Галуа, $p \subset \mathbb{Z}$ простое и $D = D_F$. $(p) = P_1^{e_1} \cdot \ldots \cdot P_g^{e_g}$, $e_1 = \ldots = e_g = e$,

$|D/P_i| = \mathbb{F}_{p^{f_i}}$, $f_1 = \ldots = f_g = f$, $efg = n$

Следствие: $[F:\mathbb{Q}] = 2$. $efg = 2$

Опр: 3 случая

1) $e = 2, f = 1, g = 1$ $\quad (p) = P^2$. $P$ — простое в $D$

наз. что $p$ разветвлено.

2) $e=1,\ f=1,\ g=2$ $\quad (p) = \underline{P}_1 \underline{P}_2,\ \underline{P}_1 \neq \underline{P}_2$

$p$ — разложимо. расщеплен

3) $e=1\quad f=2\quad g=1$, $\quad (p) = \underline{P}$ (след 2)

$p$ — ост. простым в $\mathcal{D}$

Теорема: $p \neq 2$ — пр, $\underline{P}$ — ид в $\mathcal{D}$

$\underline{P}' = \{\gamma' : \gamma \in \underline{P}\} = \{r - s\sqrt{d} : r + s\sqrt{d} \in \underline{P}\}$

1) $\left(\frac{\delta_F}{p}\right) = 0$ ($\Leftrightarrow p \mid \delta_F$) : $(p) = \underline{P}^2$

2) $\left(\frac{\delta_F}{p}\right) = 1$ ($p \nmid \delta_F$) $\quad (p) = \underline{P} \cdot \underline{P}',\quad \underline{P} \neq \underline{P}'$

3) $\left(\frac{\delta_F}{p}\right) = -1$ ($p \nmid \delta_F$) $\quad (p) = \underline{P}$

$\square$ 1) $p \mid \delta_F \qquad \delta_F = \begin{cases} 4d \\ d \end{cases} \Rightarrow p \mid d.$

Тогда $\underline{P} = (p, \sqrt{d}) = \{\alpha p + \beta\sqrt{d}\}$ — ид. в $\mathcal{D}$

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

$$\ni$$

$$(\alpha_1 p + \beta_1 \sqrt{d})(\alpha_2 p + \beta_2 \sqrt{d}) =$$

$$= p^2 \alpha_1 \alpha_2 + (\alpha_1 \beta_2 + \beta_1 \alpha_2) p \sqrt{d} + \beta_1 \beta_2 d =$$

$$= p\left(p \alpha_1 \alpha_2 + (\alpha_1 \beta_2 + \beta_1 \alpha_2)\sqrt{d} + \beta_1 \beta_2 \frac{d}{p}\right) \in$$

$$\in (p)\underbrace{\left(p, \sqrt{d}, \frac{d}{p}\right)}_{= I} \Leftarrow \gamma_1 p + \gamma_2 \sqrt{d} + \gamma_3 \frac{d}{p}, \quad \gamma_i \in \mathcal{D}$$

$$\left(p, \frac{d}{p}\right) = 1 \Rightarrow rp + s\frac{d}{p} = 1 \in I$$

$$\Rightarrow I = \mathcal{D}$$

$$(p, \sqrt{d})^2 = \mathfrak{P}^2 \subset (p) \Rightarrow (p) \mid \mathfrak{P}^2$$

$$\mathfrak{P} = (p, \sqrt{d}) \Rightarrow (p) \neq \mathfrak{P}$$

$\mathfrak{P}$ - m.i. (no $efs = 2$) $\quad (p) = \mathfrak{P}^2$

2) $\left(\frac{\delta_K}{p}\right) = 1 \Rightarrow \left(\frac{d}{p}\right) = 1 \Rightarrow \exists\, a \in \mathbb{Z}:$
$a^2 \equiv d \ (p)$

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

$\mathfrak{P}\cdot\mathfrak{P}' \subset (p)\underbrace{\left(p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p}\right)}_{=I}$

$\underbrace{a+\sqrt{d}+a-\sqrt{d}}_{2a} \in I$ , $p \in I$

4 $(p, 2a) = 1 \Rightarrow \dots \Rightarrow 1 \in I \Rightarrow I = \mathcal{O}$

$\mathfrak{P}\cdot\mathfrak{P}' \subset (p)$

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

$\Rightarrow p, 2a \in \mathfrak{P} \Rightarrow \mathfrak{P} = \mathcal{O}$ — ⨯

$\Rightarrow \mathfrak{P} \neq \mathfrak{P}'$

$\underline{P} \cdot \underline{P}' \subset (p) \iff (p) \mid \underline{P}\,\underline{P}'$

$(p) \neq \underline{P} \neq \underline{P}' \Rightarrow (p) = \underline{P} \cdot \underline{P}'$

3) $\left(\frac{\delta_F}{p}\right) = -1 \iff \left(\frac{d}{p}\right) = -1$

$\underline{P} \mid (p)$, $(p) \subset \underline{P}$

$|\mathcal{D}/\underline{P}| = p^f$, $f = 1, 2$

Ta $|\mathcal{D}/\underline{P}| = p$.

$\underset{p}{\mathbb{Z}/p\mathbb{Z}} \hookrightarrow \underset{p}{\mathcal{D}/\underline{P}} \Rightarrow \forall\, \bar{\alpha} \in \mathcal{D}/\underline{P}\ \exists\, a \in \mathbb{Z}:$

$\bar{\alpha} \equiv a \ (\underline{P})$

$\alpha = \sqrt{d}$ $\quad \exists\, a$, $\quad a \equiv \sqrt{d}\ (\underline{P})$

$\Rightarrow a^2 \equiv d\ (\underline{P})$

$a^2 - d \in P$ $\qquad P \cap \mathbb{Z} = (p) \;\Rightarrow\; a^2 - d \in (p)$

$\in \mathbb{Z}$

$$a^2 \equiv d \ (p)$$

$$\text{—} \;\; >< \;\; \left(\frac{d}{p}\right) = -1$$

$\Rightarrow \; f = 2 \qquad (p) = P$ в $\mathcal{D}$ ■

Теорема: $p = 2$

1) $2 \mid \delta_f \;\Rightarrow\; (2) = P^2$

2) $2 \nmid \delta_f \quad d \equiv 1 \ (8) \;\Rightarrow\; (2) = P P' \quad P \neq P'$

3) $2 \nmid \delta_f \quad d \equiv 5 \ (8) \;\Rightarrow\; (2) = P$

Д–. ■

Л. норм. из $\alpha \in \mathcal{D}^*$ (eq) $\Leftrightarrow$

$N\alpha = \pm 1$

Теорема: $d < 0$, $U_d = D^*$ – группа ед.

1) $U_{-1} = \{\pm 1, \pm i\}$, $|U_{-1}| = 4$

2) $U_{-3} = \{\pm 1; \pm \omega; \pm \omega^2\}$ $\omega = \frac{-1 + \sqrt{-3}}{2}$

$|U_{-3}| = 6$

3) $U_d = \{\pm 1\}$, $d < -3$, $d = -2$

$\square$ $d \equiv 2, 3\ (4)$ $D = \mathbb{Z}[\sqrt{d}]$.

$x + y\sqrt{d} \in D$ – ед $\Leftrightarrow$ $x^2 - dy^2 = \pm 1$

$x^2 + |d| y^2 = 1$

Если $|d| > 1$, то реш. $(x, y) = (\pm 1, 0)$

Если $|d| = 1$, $d = -1$, $\mathbb{Z}[i]$, реш. $(\pm 1, 0)$, $(0, \pm 1)$

$d \equiv 1 \ (4)$, $\quad D: \alpha = x + y\dfrac{-1+\sqrt{d}}{2} = \dfrac{2x - y + y\sqrt{d}}{2} = \dfrac{z + y\sqrt{d}}{2}$

$z \equiv y \ (2)$

$\alpha$ – ед $\iff$ $z^2 - dy^2 = \pm 4$, $\quad d < 0$

$\iff z^2 + |d|\, y^2 = 4$, $\quad |d| > 3$

$|d| = 3 \qquad d = -3 \qquad x^2 + 3y^2 = 4 \quad - 6$

<u>Теорема</u> (без док.) $d > 0$ и $D$

Сущ. много ед. $\exists\, \varepsilon \in D$ – фундам. ед.: $U_d = \{\pm \varepsilon^n,\ n \in \mathbb{Z}\}$

(Уравн. $x^2 - dy^2 = 1$ – уравн. Пелля.)

Теорема (Дирихле о ед.): $F$ — произв. числ. поле $[F:\mathbb{Q}] = n$.

Следствие. Гр. ед.:

$$U_D = \{ \varepsilon = \zeta \, \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}, \quad \varepsilon_1, \ldots, \varepsilon_r - \text{фунд.}, \quad \zeta \in \sqrt[n]{1}, \quad r \sim \}$$

Д-во: см. А-II

## Круговые поля.

$n \in \mathbb{Z}_{>0}$, $\zeta = \zeta_n = e^{2\pi i \frac{1}{n}}$, $x^n - 1$

Опр.) $F = \mathbb{Q}(\zeta_n)$ наз. $n$-ым круговым полем.

$x^n - 1 = (x-\zeta)(x-\zeta^2)\dots(x-\zeta^{n-1})(x-\underset{=1}{\zeta^n})$

1 $\mathbb{Q}(\zeta)$

$\mathbb{Q}(\zeta)$ — поле деления круга.

$\mathbb{Q}(\zeta)/\mathbb{Q}$ — совершенное расш.

<u>Оп</u>. $\Phi_n(x) = \prod\limits_{(a,n)=1} (x-\zeta^a)$, $\deg \Phi_n = \varphi(n)$

<u>Лемма</u>: $x^n - 1 = \prod\limits_{d|n} \Phi_d(x)$

□ Было ранее 1 вариант 2

<u>Лемма</u>: $\Phi_n \in \mathbb{Z}[x]$

□ Было

$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = G_m$

<u>Лемма</u>: $\exists\, \Theta : G_m \to U(\mathbb{Z}/m\mathbb{Z})$ — инъективный гомоморфизм, заданный условием

$\Box$ $\zeta^m = 1$, $\sigma \in G_m$, $(\sigma\zeta)^m = 1 \Rightarrow$

$(\zeta = e^{2\pi i \frac{1}{m}}, \ \zeta_a = e^{2\pi i \frac{a}{m}})$ $\quad \sigma\zeta = \zeta^{\Theta}$

$\Theta \in \mathbb{Z}/m\mathbb{Z}$. $\quad \Theta = \Theta(\sigma)$

$\tau = \sigma^{-1}$ $\quad \tau\sigma = id$ $\quad (\tau\sigma)(\zeta) = \zeta$

$$\tau(\sigma(\zeta)) = \tau(\zeta^{\Theta(\sigma)}) = (\tau\zeta)^{\Theta(\sigma)} = \zeta^{\Theta(\tau)\Theta(\sigma)}$$

$\Rightarrow \Theta(\tau)\Theta(\sigma) \equiv 1 \ (m)$

$\sigma_1, \sigma_2 \in G_m$ $\quad \sigma_1(\sigma_2(\zeta)) = (\sigma_1\sigma_2)(\zeta) = \zeta^{\Theta(\sigma_1\sigma_2)} = \zeta^{\Theta(\sigma_1)\Theta(\sigma_2)} \Rightarrow \Theta(\sigma_1\sigma_2) \equiv \Theta(\sigma_1)\Theta(\sigma_2)\ (m)$

Инъективность: $\Theta(\sigma) \equiv 1 \ (m)$ $\quad \sigma\zeta = (\zeta)^{\Theta(\sigma)} = \zeta$

$\sigma = id$

$\Theta$ гом. на $U(\mathbb{Z}/m\mathbb{Z})$ ■

$\mathbb{Q}(\zeta)/\mathbb{Q}$ — нормальное,

расш. Галуа

**Теорема**: $\mathbb{Q}(\zeta)/\mathbb{Q}$ — расш. Галуа

$[\mathbb{Q}(\zeta):\mathbb{Q}] = |G_n|$

**Следствие**: $|G_n| \geq \varphi(n)$ $\Rightarrow$ $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$ ■

**Лемма**: $\Phi_n \in \mathbb{Z}[x]$

$\Rightarrow$ $\sigma\Phi_n(x) = \sigma\left(\prod_{(a,n)=1}(x-\zeta^a)\right) =$

$= \prod_{(a,n)=1}(x-\zeta^{a\theta(\sigma)}) = \Phi_n(x)$

$\Rightarrow$ $\Phi_n \in \mathbb{Q}[x]$, $\in \mathbb{Z}[x]$ ■

Теорема: $\Phi_n(x)$ непр. $/\mathbb{Q}$ $(/\mathbb{Z})$

Идея:

□ $\Phi_n$ — мин. многоч. $\zeta$. зн. $\mathbb{Q}(\zeta)$

Пусть $f$ — мин. многоч. $\zeta$, $p$ — пр.

$(p, n) = 1$

$D = D_{\mathbb{Q}(\zeta)}$ $\quad (p) \subset P$ — пр. ид. $D$, над $p$

$f$ мин. $\zeta$ — кор. $x^n - 1 \Rightarrow f \mid x^n - 1$

$\Rightarrow$ все корни $f$ — кор. $x^n - 1$

т.е. $\sqrt[n]{1}$ (дискр. мн. $x^n - 1$)

$$\Delta = \prod_{i<j} (\zeta^i - \zeta^j)^2 = \pm \prod_{i \neq j} (\zeta^i - \zeta^j) = \pm \prod_{i \neq j} \zeta^i (1 - \zeta^{j-i})$$

$$= \pm \prod_i \zeta^i \prod_{k \neq 0} (1 - \zeta^k)$$

$$\frac{x^m - 1}{x - 1} = \prod_{k \neq 0} (x - \zeta^k)$$

$$= x^{n-1} + x^{n-2} + \dots + 1$$

Take $x = 1$, $m = \prod_{k \neq 0} (1 - \zeta^k)$

$$\Delta = \pm \prod_i (\zeta^i \cdot m) = \pm m^m \underbrace{\prod_i \zeta^i}_{=1} = \pm m^m$$

$|\Delta| = m^m$.

$(p, m) = 1$. $\zeta^p$ - non root $f$:

when $f(\zeta^p) \neq 0$

$$f(x) = \underbrace{(x - \zeta_1) \dots (x - \zeta_k)}_{\sqrt[m]{1}} \qquad \zeta_1 = \zeta = e^{2\pi i \frac{1}{m}}$$

$f(\zeta^p) = \prod($[illegible] [illegible] $(\zeta^i - \zeta^{j}))$

$\Rightarrow f(\zeta^p) \mid \Delta$ в $D$

$\Rightarrow f(\zeta^p) \mid m^n$ в $D$

$f(x^p) \equiv f(x)^p \ (p) \qquad p \mid f(x^p) - f(x)^p$

$f(\zeta^p) \equiv \underbrace{f(\zeta)^p}_{=0} \ ((p))$ в $D$

в $D \quad p \mid f(\zeta^p) \mid m^n$

$\Rightarrow p \mid n^n$ в $D \Rightarrow p \mid n^n$ в $\mathbb{Z}$

$-$ $\times$ $(p, n) = 1$

т.о. $f(\zeta^p) = 0$

Если $(a, n) = 1$ $\quad a = \prod p^{\nu_p}$ $\quad (p, n) = 1$

$\Rightarrow$ $\xi^a$ — корень многочлена $f$

$\deg f \geq \varphi(n)$

$\Phi_n(\xi) = 0 \Rightarrow f \mid \Phi_n \Rightarrow \deg f \leq \varphi(n)$

$\deg f = \deg \Phi_n = \varphi(n)$

$$f = \Phi_n = \prod_{(a,n)=1} (x - \xi^a)$$

$\Rightarrow \Phi_n$ неприв. $\blacksquare$

<u>Следствие</u>: 1) $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$

2) $\Theta : G_n \to U(\mathbb{Z}/n\mathbb{Z})$ — изом.

Теорема: $\mathcal{D} = \mathbb{Z}[\zeta]$

( $p$ нечёт., $m = p$ — пр. )

$\mathbb{Q}(\alpha)$, $\mathcal{D}_{\mathbb{Q}(\alpha)} \neq \mathbb{Z}[\alpha]$

Лемма: $p \nmid m$, $f$ — пор. $p$ mod $m$

( $p^f \equiv 1\ (m)$, $f$ — наим. ). В $\mathcal{D}$

$(p) = \mathfrak{p}_1 \dots \mathfrak{p}_g$, $\mathfrak{p}_i$ — степ. $f$

$$g = \frac{\varphi(m)}{f}$$

□ — ■

Лемма: $p = m$ $\mathfrak{p} = (1-\zeta)$ $\left(\zeta = \zeta_p = e^{2\pi i \frac{1}{p}}\right)$

$\mathfrak{p}$ — пр. в $\mathcal{D}$ $(p) = \mathfrak{p}^{p-1}$ □ — ■

$\mathbb{Z}[i\mathbb{R}]$.

$d<0$ $\qquad i, \quad \omega, \quad \frac{-1+\sqrt{-3}}{2}$

$\qquad 4 \qquad 6 \qquad\qquad 2$

[illegible] [illegible] – [illegible]. [illegible].

Теорема (Кронекер–Вебер) $\forall$ $F/\mathbb{Q}$ — [illegible], $Gal(F/\mathbb{Q})$ — [illegible],

$\exists\, n$ $\quad F \subset \mathbb{Q}(\zeta_n)$, $\zeta_n = e^{2\pi i \frac{1}{n}}$

$\mathbb{Q}(\zeta_n) / F / \mathbb{Q}$.

$\mathbb{C}$ $\qquad \mathcal{D}$ $\qquad \mathbb{R}^n$

$\mathbb{Z}\langle i\rangle$