§2. Прості елементи та однозначність факторизації

R область цілісності

$a, b \in R$, $a \neq 0$

$a \mid b \iff \exists c \in R : b = ac$

Оз-ня $r \in R$ наз-ся **незвідним** якщо $r \neq 0$, $r \notin R^\times$, та

$a \mid r \Rightarrow a \in R^\times$ або $a \in R^\times r$

одиниця кільця — асоційований з r ел-т

Приклад: $R = k[x]$

незвідні многочлени – ті, що не розкладаються на добуток несталих многочленів ($\deg > 0$) меншого степеня

$R^\times = k^\times$

$k = \mathbb{Q}$ критерій Ейзенштейна

$f(x) = a_0 + a_1 x + \ldots + a_n x^n$

$a_i \in \mathbb{Z}$ $\forall i$ $\quad a_n \neq 0$

якщо $\exists$ просте число p

що $p \nmid a_n$, $p \mid a_i$ $i = 0, \ldots, n-1$, $p^2 \nmid a_0$

тоді $f(x)$ незвідний в $\mathbb{Q}[x]$

(доведемо пізніше у курсі)

Озн-ня $r \in R$ наз-ся **простим** якщо $r \neq 0$, $r \notin R^{\times}$ та $r \mid ab \Rightarrow r \mid a$ або $r \mid b$.

Вправа: покажіть, що простий ел-т є незвідним. Подайте приклад кільця R та елемента $r \in R$ який є незвідним але не є простим.

Тв-ня 1 Якщо R це ОГІ тоді кожен незвідний ел-т є простим.

Дов-ня $r \in R$ незвідний. Нехай $r \mid ab$ та $r \nmid a$.

незвідність $r \Rightarrow$ єдині спільні дільники r і a це одиниці кільця

$\langle r, a \rangle = R \Rightarrow$

$\langle rb, ab \rangle = \langle b \rangle$

$r \mid ab \Rightarrow \langle rb, ab \rangle \subset \langle r \rangle$

$\Leftrightarrow r \mid b$ $\boxtimes$

Тобто в ОГІ поняття незвідного і простого елемента співпадають.

Нехай R це ОГІ.
Нехай $\mathcal{P}$ це така множина простих ел-тів в R що:

- кожен простий ел-т в R асоційований з деяким ел-том $\mathcal{P}$
- ніякі два ел-ти $\mathcal{P}$ не є асоційованими

<u>Теорема 2</u> Кожен ненульовий ел-т $0 \neq r \in R$ може бути єдиним способом записаний як добуток

$$r = u \prod_{p \in \mathcal{P}} p^{e_p},$$

де $e_p \in \mathbb{Z}_{\geq 0}$, $e_p = 0$ для майже всіх p, $u \in R^{\times}$.

<u>Лема 3</u> Кожен зростаючий ланцюг ідеалів

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \ldots$$

є скінченним, тобто $\exists k$ т.щ. $\langle a_k \rangle = \langle a_{k+l} \rangle$ $\forall\, l = 0, 1, 2, \ldots$

<u>Дов-ня:</u> Нехай $I = \bigcup_{i=0}^{\infty} \langle a_i \rangle$.
Легко перевірити що I - ідеал.
$R \in$ ОГІ $\Rightarrow$ $I = \langle a \rangle$.
$a \in I \Rightarrow \exists k$ т.щ. $a \in \langle a_k \rangle$
$\Rightarrow I = \langle a \rangle \subset \langle a_k \rangle \Rightarrow I = \langle a_k \rangle$ $\boxtimes$

Лема 4 Кожен $a \in R$, $a \neq 0$, $a \notin R^\times$ є добутком незвідних елементів.

Дов-ня Якщо a незвідний – твердження для нього виконується.

Якщо ні, тоді $a = a_1 b_1$ з $a_1, b_1 \notin R^\times$. Ми хочемо показати на початку, що a ділиться на деякий незвідний ел-т. Якщо a_1 – незвідний, ціе все так. Якщо ні, то $a_1 = a_2 b_2$, $a_2, b_2 \notin R^\times$. І так далі.

$a_{k+1} \mid a_k \quad \forall k$

$(a) \subset (a_1) \subset (a_2) \subset \ldots$

Лема 3 $\Rightarrow$ цей ланцюг є скінченним $\Rightarrow$ $\exists k$ т. щ. a_k є незвідним.

Ми довели, що a ділиться на незвідний ел-т. Нехай $a = c_1 d_1$, де c_1 незвідний. Якщо d_1 незвідний, мету досягнено. Інакше $d_1 = c_2 d_2$ де c_2 є незвідним. І т. д.

$(a) \subset (d_1) \subset (d_2) \subset \ldots$ є скінченним, тобто $\exists k$ т. щ. $d_k \in R^\times$. $\boxtimes$

Лема 5 Нехай $p \in R$ простий і $a \in R, a \neq 0$. Тоді $\exists\, n \in \mathbb{Z}_{\geq 0}$ т.щ.

$$p^n \mid a \quad \text{і} \quad p^{n+1} \nmid a.$$

Дов-ня: Якщо тв-ня леми не виконується то

$$a = p^m b_m, \quad \forall m \geq 0$$

Тоді $p b_{m+1} = b_m$ і

$\langle b_1 \rangle \subset \langle b_2 \rangle \subset \dots$ є нескінченним, суперечність. $\boxtimes$

Позначення: $n = \mathrm{ord}_p a$
"порядок p в a"

Властивості (вправа):

- $a, b \neq 0$
  $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$
- p, p' не асоційовані прості, тоді
  $\mathrm{ord}_p(p') = 0$
- $\forall\, v \in R^\times \quad \mathrm{ord}_p(v) = 0$

Дов-ня Теореми 2

Лема 4 $\Rightarrow$

$$r = u \prod_{p \in \mathcal{P}} p^{e_p} \qquad (*)$$

Єдиність? Для кожного $p \in \mathcal{P}$ застосуємо ord_p до $(*)$

$\Rightarrow e_p = \mathrm{ord}_p r$ $\boxtimes$

<u>Озн-ня</u> Область цілісності R, у якій кожен ненульовий ел-т може бути представлений як добуток простих елементів однозначно з точністю до порядку та асоційованих ел-тів (див. Теорему 2 для точного формулювання) наз-ся <u>областю однозначної факторизації</u> (ООФ).

Теорема 2 стверджує що кожна ОГІ це ООФ.

Приклади: $\mathbb{Z}$, $k[x]$ це ООФ

$k[x_1, \dots, x_n]$ це ООФ але не ОГІ (коли $n > 1$)

<u>Теорема</u> (з комутативної алгебри): якщо R це ООФ то $R[x]$ це також ООФ.

Скоро ми сконструюємо кільця, які не є ООФ.

§3. Алгебраїчні числа

Оз-ня $\xi \in \mathbb{C}$ наз-ся алгебраїчним числом якщо $\exists\, f \in \mathbb{Q}[x], f \neq 0$ т.щ. $f(\xi) = 0$.

Розглянемо

$$I_\xi = \{ f \in \mathbb{Q}[x] : f(\xi) = 0 \}$$

ідеал в $\mathbb{Q}[x]$

$\Rightarrow$

$\exists!$ нормований многочлен g т.щ.

$$I_\xi = \langle g \rangle$$

Ясно що g це многочлен мінімального степеня в $I_\xi \setminus \{0\}$.

Оз-ня $g(x)$ наз-ся мінімальним многочленом (або мінімальним рівнянням) алг. числа ξ.

Тв-ня 1 Мінімальний многочлен є незвідним.

Дов-ня: Якщо це не так, то
$$g(x) = g_1(x)\, g_2(x)$$
так що $0 < \deg(g_i) < \deg(g)$, $i = 1, 2$.

$0 = g(\xi) = g_1(\xi) \cdot g_2(\xi) \Rightarrow g_1(\xi) = 0$ або $g_2(\xi) = 0$. Суперечність $\boxtimes$

Приклади:

$\xi = \sqrt[3]{7}$ $\quad g(x) = x^3 - 7$

незвідний за критерієм Ейзенштейна для $p = 7$

$\Rightarrow$ мінімальний

$\xi = \sqrt{10}$ $\quad g(x) = x^2 - 10$

— // — $p = 2$ і $p = 5$

$\xi = \frac{1}{\sqrt{6}}$ $\quad g(x) = x^2 - 1/6$

$6x^2 g(1/x) = -x^2 + 6$

незвідний за кр-єм Ей-на для $p = 2$ або 3

$\Rightarrow$ g є незвідний

$\Rightarrow$ мінімальний

Позначення: $\overline{\mathbb{Q}} \subset \mathbb{C}$

алгебраїчні числа

Вправа: знайдіть мінімальний многочлен $1 + \sqrt{2} + \sqrt{3}$.

Озн-ня: Алг. число $\xi \in \overline{\mathbb{Q}}$ наз-ся <u>цілим</u> якщо воно задовольняє деякому нормованому рівнянню

$$\xi^n + a_{n-1}\xi^{n-1} + \ldots + a_1\xi + a_0 = 0$$

з $a_i \in \mathbb{Z}$, $i = 0, \ldots, n-1$.

Тобто $\sqrt[3]{7}, \sqrt{10}$ є цілими.

Чи є цілим $1/\sqrt{6}$?

Тв-ня 2 Мінімальне рів-ня алг. цілого числа є нормованим рів-ням з цілими коефіцієнтами.

Оз-ня Многочлен $f \in \mathbb{Z}[x]$ наз-ся **примітивним** якщо його коефіцієнти є взаємно-простими.

$$f = \sum_{i=0}^{n} a_i x^i$$

$$(a_0, \dots, a_n) = 1$$

Лема Гаусса Добуток примітивних м-ів є примітивним. (вправа)

Дов-ня Тв-ня 2 Нехай

$$f(x) = x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$$

та $f(\xi) = 0$. Тоді

$$f(x) = h(x)\, g(x)$$

мінімальний для ξ

Нехай

$$h(x) = \frac{1}{A} H(x)$$

$$g(x) = \frac{1}{B} G(x)$$

це H, G примітивні, $A, B \in \mathbb{Z}$

це Н.С.К. знаменників коефіцієнтів $h(x)$ і $g(x)$ відповідно

$AB\, f(x) = H(x)G(x)$

л. Гаусса $\Rightarrow$ $AB\, f(x)$ є примітивним

$\Rightarrow AB = \pm 1$

$\Rightarrow g(x) \in \mathbb{Z}[x]$ (і є примітивним).

$\boxtimes$

Поз-ня: $\overline{\mathbb{Z}}$ алг. цілі числа

$$\begin{array}{ccccc} \overline{\mathbb{Z}} & \subset & \overline{\mathbb{Q}} & \subset & \mathbb{C} \\ \cup & & \cup & & \\ \mathbb{Z} & \subset & \mathbb{Q} & & \end{array}$$

Озн-ня: Числа в $\mathbb{C} \setminus \overline{\mathbb{Q}}$ наз-ся трансцендентними.

Тв-ня 3 Якщо $\xi_1, \xi_2 \in \overline{\mathbb{Q}}$ то $\xi_1 + \xi_2$, $\xi_1 \xi_2 \in \overline{\mathbb{Q}}$.

Якщо $\xi_1, \xi_2 \in \overline{\mathbb{Z}}$, то $\xi_1 + \xi_2$, $\xi_1\xi_2 \in \overline{\mathbb{Z}}$.

Лема 4 Нехай $\xi \in \mathbb{C}$ і для деякого $n \geq 1$ та $\theta_1, \dots, \theta_n \in \mathbb{C}$ не всіх нульових виконується

$\xi\theta_1 = a_{1,1}\theta_1 + \ldots + a_{1,n}\theta_n$

$\xi\theta_2 = a_{2,1}\theta_1 + \ldots + a_{2,n}\theta_n$

$\ldots$

$\xi\theta_n = a_{n,1}\theta_1 + \ldots + a_{n,n}\theta_n$

де всі n^2 коефіцієнтів $a_{i,j} \in \mathbb{Q}$. Тоді $\xi \in \overline{\mathbb{Q}}$. Більше того, якщо $a_{i,j} \in \mathbb{Z}$ тоді $\xi \in \overline{\mathbb{Z}}$.

<u>Дов-ня</u> $\xi\vec{\theta} = A\vec{\theta}$

$\vec{\theta} \neq \vec{0} \Rightarrow \det(\xi - A) = 0$

$\det(x - A) = x^n + \ldots$

є нормованим рівнянням для ξ з коефіцієнтами в $\mathbb{Q}$ / $\mathbb{Z}$ відповідно. $\boxtimes$

Дов-ня тв-ня 3

Нехай

$$\xi_1^m + a_{m-1}\xi_1^{m-1} + \ldots + a_0 = 0$$

$a_i \in \mathbb{Q} / \mathbb{Z}$

$$\xi_2^k + b_{k-1}\xi_2^{k-1} + \ldots + b_0 = 0$$

$b_j \in \mathbb{Q} / \mathbb{Z}$

Застосуємо лему 4

з $n = k \cdot m$ та

$$\Theta_{s,t} = \xi_1^s \xi_2^t, \quad 0 \leq s \leq m-1, \quad 0 \leq t \leq k-1$$

...

$\boxtimes$

Наслідок: $\overline{\mathbb{Z}}$ це кільце

$\overline{\mathbb{Q}}$ це поле

Вправа: $m \in \mathbb{Z}$ $m \neq 0, 1$

вільне від квадратів

Покажіть що

$K = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$

є полем. Опишіть кільце цілих елементів цього поля

$$\mathcal{O}_K = K \cap \overline{\mathbb{Z}}.$$