Алгебра-III | НМУ | Лекция-2 | 15.09.2020

<u>План:</u> - алгебраические мн-ва (в $\mathbb{C}^n$)
- Теорема Гильберта о нулях
- Факториальные кольца: Лемма Гаусса, Критерий Эйзенштейна

Рассмотрим кольцо мн-нов $\mathbb{C}[x_1,\dots,x_n]$, про него можно думать, как про формальный алгебраический объект, а можно, как про кольцо полиномиальных ф-ий в $\mathbb{C}^n$, потому как для каждой точки $\overline{p}=(p_1,\dots,p_n)\in\mathbb{C}^n$ корректно определено значение

$$ev:\ \mathbb{C}[x_1,\dots x_n]\to\mathbb{C}$$
$$x_i\to p_i$$
$$f(x_1,\dots,x_n)\to f(p_1,\dots,p_n).$$

Что можно сопоставить подмн-ву $M\subset\mathbb{C}^n$

$\rightsquigarrow$ алг-ру ф-ий на M $=\mathbb{C}[x_1,\dots,x_n]/I(M)$ ← ф-ии, зануляющиеся в M.

<u>Имеем:</u>

$$\begin{pmatrix}\text{Идеалы}\\ \text{в } \mathbb{C}[x_1,\dots,x_n]\end{pmatrix}\ \underset{\mathfrak{a}\mapsto V(\mathfrak{a})}{\overset{I(M)\leftarrow M}{\rightleftarrows}}\ \begin{pmatrix}\text{подмн-ва}\\ \text{в } \mathbb{C}^n\end{pmatrix}$$

$V(\mathfrak{a}):=\{(p_1,\dots,p_n)\in\mathbb{C}\ |\ \forall f\in\mathfrak{a}\ \ f(p_1,\dots,p_n)=0\}$ – мн-во общих нулей идеала.

Вспомним, что кольцо $\mathbb{C}[x_1,\dots,x_n]$ – нётерово.
поэтому любой идеал порождается конечным набором мн-нов
и мы приходим к естественному

<u>Опр</u> Мн-во M совместных нулей конечного набора полиномов $f_1,\dots,f_m$ называется (замкнутым) алгебраическим подмножеством в $\mathbb{C}^n$.

<u>Замечание</u> Введённая таким образом топология называется топологией Зарисского.

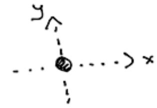
Понятно, что

$V(I(M))\supseteq M$, Однако это далеко не всегда равенства.

$I(V(\mathfrak{a}))\supseteq\mathfrak{a}$

Пример. (xy) $\longleftrightarrow$  $(y) = I(M)$ $\longleftarrow$ 

(x^2y)

(x,y) $\longleftrightarrow$  $(1) = I(M) \longleftarrow$

Опр. $r(\mathfrak{a}) := \{f \mid f^k \in \mathfrak{a}\}$, тогда $r(\mathfrak{a})$ — радикал. идеала $\mathfrak{a}$. (это тоже идеал)

Однако эти отображения $I(-)$, $V(-)$ взаимно обратны на своих образах.

Теорема Гильберта о нулях

(i) $V(\mathfrak{a}) = \varnothing \iff \mathfrak{a} \ni 1$ (т.е. $\mathfrak{a} = \mathbb{C}[x_1,\dots,x_n]$)

(ii) Если f обращается в 0 во всех точках $V(\mathfrak{a})$, то $\exists k: f^k \in \mathfrak{a}$.

т.е. $I(V(\mathfrak{a})) = r(\mathfrak{a})$.

Д-во (Трюк Рабиновича)

(Утв из аксиомы выбора следует, что $\forall \mathfrak{a}$ $\exists$ максимальный идеал $\mathfrak{m} \supset \mathfrak{a}$).

Замеч. Идеал $\mathfrak{m} \subset R$ - максимальный (по включению) $\iff$ $R/\mathfrak{m}$ — поле.

Остаётся д-ть, что $\mathbb{C}[x_1,\dots,x_n]/\mathfrak{m}$ - поле

$$\mathbb{C} \hookrightarrow \mathbb{C}[x_1,\dots,x_n]/\mathfrak{m} \longrightarrow \mathbb{F}$$

$\mathfrak{m}$ имеет ноль в $\mathbb{F}^n$ (образ точки $(x_1,\dots,x_n) \in \mathbb{F}^n \Rightarrow$

Достаточно показать, что $\mathbb{F} = \mathbb{C}$.

Предположим обратное, т.е. $\mathbb{F} \neq \mathbb{C}$, возьмём $a \in \mathbb{F} \setminus \mathbb{C}$.

$\Rightarrow f(a) \neq 0$ $\forall f \in \mathbb{C}[t]$ (в виду алг. замкнутости поля $\mathbb{F}$)

$\Rightarrow$ эл-ты вида $\frac{1}{a-\lambda}$, $\lambda \in \mathbb{C}$ линейно независимы над $\mathbb{C}$.

$\Rightarrow \dim_{\mathbb{C}} \mathbb{F}$ — несчётно, однако $\mathbb{C}[x_1,\dots,x_n]$ порождается над $\mathbb{C}$ счётным базисом.

(Импликация: (i) $\Rightarrow$ (ii))

Пусть f обр. в ноль во всех точках $V(\mathfrak{a})$.

Тогда рассмотрим $\underset{\mathfrak{a}}{\underset{\cup}{\mathbb{C}[x_1,\dots,x_n]}} \subset \mathbb{C}[x_1,\dots,x_n,t]$

$$\mathfrak{b} = (\mathfrak{a}, \underbrace{1-tf}_{g})$$

Мн-во общих нулей $V(\mathfrak{b}) \subset \mathbb{C}^{n+1}$ - пустое, т.к. если $(\bar{x}, p) \in V(\mathfrak{b})$, то $f(\bar{x}) = 0 \Rightarrow g(\bar{x}, p) = 1$.

$\Rightarrow \exists\ g_0, \dots, g_s \in \mathbb{C}[x_1, \dots, x_n, t]$
$f_1, \dots, f_s \in \mathfrak{a}$, такие что $\boxed{g_0 \cdot (1 - tf) + g_1 f_1 + \dots + g_s f_s = 1}$

это равенство в $\mathbb{C}[x_1, \dots, x_n, t]$,

и подставим вместо t эл-нт $\frac{1}{f(x)} \in \mathbb{C}(x_1, \dots, x_n)$ (кольца рациональных ф-ций)

Имеем $g_0(x, \frac{1}{f(x)}) \cdot \underset{\overset{\shortparallel}{0}}{(1 - \frac{1}{f} f)} + g_1(x, \frac{1}{f}) \cdot f_1 + \dots + g_s(x, \frac{1}{f}) f_s = 1$

Домножаем на знаменатель имеем $\mathfrak{a} \ni \sum f_i(x) \tilde{g}_i(x) = f^k$

$\Rightarrow f^k \in \mathfrak{a}$. $\square$

С-ие Идеал $(x_i - a_i)$ — максимален — и все максимальные идеалы таковы

Д-во $\mathbb{C}[x_1, \dots, x_n] / (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n) \simeq \mathbb{C} \Rightarrow$ он максимален.

Если $\mathfrak{a} \subset \mathbb{C}[x_1, \dots, x_n]$ - максимален, то $V(\mathfrak{a}) \neq 0$
$\Rightarrow \exists p \in V(\mathfrak{a})$

$\Rightarrow m := (x_1 - p_1, \dots, x_n - p_n) \supset r(\mathfrak{a}) \supset \mathfrak{a}$.

Лекция 3

22.09.2020

Итого $\left(\begin{array}{c} \text{радикальные} \\ \text{идеалы в} \\ \mathbb{C}[x_1, \dots, x_n] \end{array} \right) \xleftrightarrow{1:1} \left(\begin{array}{c} \text{Алгебраические} \\ \text{подмн-ва в } \mathbb{C}^n \end{array} \right)$

Теор. $r(\mathfrak{a}) = \bigcap_{p \supset \mathfrak{a}} p$. Т.е. есть, радикал идеала совпадает с пересечением всех простых, его содержащих.

Д-во: $p \supset \mathfrak{a} \Rightarrow p \supset r(\mathfrak{a}) \Rightarrow \bigcap_{p \supset \mathfrak{a}} p \supset r(\mathfrak{a})$.

Пусть $x \in \bigcap_{p \supset \mathfrak{a}} p \setminus r(\mathfrak{a})$.
Покажем, что максимальный идеал b, не содержащий $1, x, x^2, \dots$ является простым.
Пусть $y \cdot y' \in b$, но $y, y' \notin b$.
из максимальности следует, что $\exists\ k, m$, такие что

$b + yz = x^k$
$b' + y'z' = x^m$ $\Rightarrow (b + yz)(b' + y'z') = x^{k+m} \notin b$

Пример радикального идеала:

простой p

Опр. идеал p — простой
Если R/p - область целостности
$\Leftrightarrow ab \in p \Rightarrow \left[\begin{array}{l} a \in p \\ b \in p. \end{array} \right.$

Поэтому $f^k \in p \Rightarrow f \in p$.

Аналогично Если $p_1, \dots, p_k$ — набор простых, то $\mathfrak{a} = p_1 \cap \dots \cap p_k$ — радикальный.

Геометрически имеем

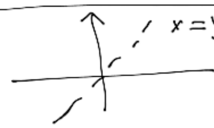
$$V(p_1\cap p_2) = V(p_1)\cup V(p_2)$$

↑ неприводимые компоненты.

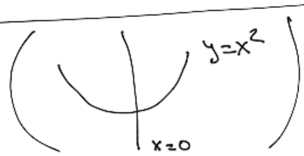
$p \supset p_1\cap p_2 \Rightarrow \left[\begin{matrix} p\supset p_1\\ p\supset p_2\end{matrix}\right.$

т.к. если $a_i \in p_i\setminus p \Rightarrow a_1 a_2 \in p_1 p_2$, $\notin p$

Опр. алгебр. подмн. $X\subset \mathbb{C}^n$ называется приводимым, если оно представляется в виде объединения двух замкн. собственных подмножеств.

В частности, прямая  $x=y$ — явл. неприв

И вообще, если $f\in\mathbb{C}[x_1,\dots,x_n]$ — неприводим, то и соотв. мн-во $V(f)$ — неприводимо.

Пример $I\Big($  $\Big) = (x)\cap(y-x^2) = (x\cdot(y-x^2))$.

↑ главный идеал.

Такое возможно сделать, поскольку в кольце $\mathbb{K}[x_1,\dots,x_n]$ имеется **однозначное разложение на множители.**

Опр. Область целостности с однозначным разложением на множители наз-ся факториальным кольцом (Unique Factorization domain).

Напоминание: $f = u\cdot p_1\cdot\ldots\cdot p_n = v\cdot q_1\cdot\ldots\cdot q_m$, где u,v — обратимые, а p_i, q_j — неразложимые

то $m=n$ и $\exists\,\sigma\in S_n:\ p_i=\varepsilon_i q_{\sigma(i)}$, ε_i — обратимы.

Пример $\mathbb{Z}$, $\mathbb{K}[x]$ и вообще евклидовы кольца являются факториальными,

а $\mathbb{Z}[\sqrt{-5}]$ не факториально, т.к. $2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$

Цель Д-ть, что $\mathbb{K}[x_1,\dots,x_n]$ — факториально.

Теор. Если R целостное и у каждого ненулевого эл-та $a \in R$ имеется хотя бы одно разложение в конечное произведение неразложимых. Тогда R - факториально, если и только если $\forall$ неразложимого $p \in R$, главный идеал (p) - простой.

Д-во: $ab \vdots p \Rightarrow \left[\begin{matrix} a \vdots p \\ b \vdots p \end{matrix}\right.$ - это простота идеала.

(далее упражнение завершить д-во).

$\boxed{\text{В факториальном кольце есть НОД и НОК.}}$

Опр. Пусть R - факториальное кольцо.

$f \in R[x]$, тогда содержанием $d(f) := \text{НОД}(a_0, \ldots, a_n)$

Если $d(f)$ - обратим, то f - примитивный.

Теор. (Лемма Гаусса) $d(fg) = d(f) \cdot d(g) \cdot \varepsilon$ ← обратимый $\quad \forall f, g \in R[x]$

если R - факториально.

Д-во: пусть примитивные $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, пусть p - неразложимый $\Rightarrow$ (p) - простой. Возьмём $k = \min_i \{a_i \mid a_i \notin (p)\}$, $\ell = \min_j \{b_j \mid b_j \notin (p)\}$.

тогда коэф при $k+\ell$ в $f(x) \cdot g(x) \equiv a_k b_\ell \pmod p \notin p$.

$\Rightarrow fg$ - тоже примитивный.

Иначе содерж. можно вынести.

Сл-ие R - факториальное кольцо, $\mathbb{F}$ - поле частных

тогда мн-н $f(x) \in R[x]$ неразложим в произв. мн-нов меньшей степени

$\Updownarrow$

$f(x) \in \mathbb{F}[x]$ - неразложим.

Теор. R - факториально $\Rightarrow R[x]$ - факториально

Д-во: Пусть f - неразложим в $R[x]$, тогда или $f \in R$ и неразложим

$\Rightarrow$

$R[x]/(p) \simeq R/(p)[x]$ - область целости.

$\Rightarrow$ простой (p).

или $\deg(f) \geq 1$ и f - примитивный.

тогда f – неразложим в $\mathbb{F}[x]$, которое факториально.

$\Rightarrow$ Имеем $gh \vdots f$ в $R[x]$ $\Rightarrow$ $\left[\begin{matrix} g \vdots f \\ h \vdots f \end{matrix}\right.$ в $\mathbb{F}[x]$ $\Rightarrow$ $\left[\begin{matrix} g \vdots f \\ h \vdots f \end{matrix}\right.$ в $R[x]$.

Критерий Эйзенштейна $f(x) = a_n x^n + \ldots + a_0$ $\begin{matrix} a_i \vdots p \quad \forall i < n \\ a_0 \not\vdots p^2 \end{matrix}$ $\Rightarrow$ $f(x)$ – неприводим.

Д-во: Мн-н $f(x)$ приводим в $R[x]$ $\Leftrightarrow$ приводим в $\mathbb{F}[x]$.

$\Leftrightarrow$ $f(x) = g(x) \cdot h(x)$, $\in R[x]$.

Возьмём редукцию по модулю p.

имеем $a_n x^n = \overline{g(x)} \cdot \overline{h(x)} \in R/_p[x]$

$\Rightarrow$ $\overline{g(x)} = \bar{a} \cdot x^k$, $\bar{h}(x) = \bar{b} x^l$ $\Rightarrow$ все коэф-ты $g(x)$ и $h(x)$ кроме старших делятся на p.

$\Rightarrow$ $a_0 \vdots p^2$.

Пример 0 $f(x) = \dfrac{x^p - 1}{x-1} = x^{p-1} + \ldots + 1$, После замены $y = x+1$

имеем $\dfrac{(y+1)^p - 1}{y}$ – применяем критерий Эйзенштейна.

Пример 1 $y^2 = x^3 + 1$ – кубическая кривая

$= (x+1) \cdot (x^2 - x + 1)$.

Применяем критерий Эйзенштейна в $(\mathbb{C}[x])[y]$

простой – $(x+1) \in \mathbb{C}[x]$.

К сожалению, нет общего метода док-ва неприводимости мн-на в $\mathbb{F}[x]$, тем более в $\mathbb{F}[x_1, \ldots, x_n]$.