(1) Кольца целых алгебраических элементов

1. Кольца, модули, идеалы, подмодули

У нас R – (ассоц.) комм. кольцо с 1.

R^+ – аддитивная группа кольца, R^* – группа обр. эл-тов (мультипл.)

Поскольку $A \leq R \Leftrightarrow A$ – кольцо отн-но $+|_A, \cdot|_A$

Идеал $I \trianglelefteq R \Leftrightarrow I^+ \leq R^+$ и $aI \subseteq I \ \forall a \in R$.

$I \trianglelefteq R \Rightarrow R/I = \{a+I \mid a \in R\}$ – фактор-кольцо.

Гом-зм $f: A \to B \Leftrightarrow f(x+y)=f(x)+f(y)$, $f(xy)=f(x)f(y)$ и $f(1)=1$.

Т-ма о гом-зме: $f: A \to B$ – гом-зм колец, тогда $\varphi: a+\operatorname{Ker} f \mapsto f(a)$ – изоморфизм колец $A/\operatorname{Ker} f$ и $f(A)$.

Идеал $I \trianglelefteq R$ **максимален**, если $\forall J \trianglelefteq R$
из $I \subseteq J \Rightarrow I = J$

Упр $I \trianglelefteq R$ макс $\Leftrightarrow R/I$ – поле. В частности, $M \trianglelefteq_{max} \mathbb{Z} \Leftrightarrow M$ – простое

Опр Кольцо R наз-ся **локальным**, если в нем только один максим. идеал

Пример Поле – локальное кольцо, т.к. 0 – ед. макс. идеал

$\mathbb{Z}$ не локально, т.к. $p\mathbb{Z} \trianglelefteq_{max} \mathbb{Z}$ $\forall$ простого p

Предл 1 Пусть M – макс. идеал в кольце R.
R локально $\Leftrightarrow$ $1+x$ обратим $\forall x \in M$

Упр 1 а) Д-то пр. 1. б) $\mathbb{Z}_n$ локально $\Leftrightarrow n = p^k$ для простого p.

Кольцо $R = R_1 \oplus \dots \oplus R_k$, где $R_i \leq R$, если

(1) $R^+ = R_1^+ \oplus \dots \oplus R_k^+$ и (2) $R_i R_j = 0$ при $i \neq j$

Зам. Прибыл. (1) условие (2) $\Leftrightarrow R_i \trianglelefteq R$ $\forall i = 1 \dots k$.

При этом $(x_1 + \dots + x_k)(y_1 + \dots + y_k) = x_1 y_1 + \dots + x_k y_k$

Обратно, если $R_1, \dots R_k$ – произв. кольца, то $R_1 \oplus \dots \oplus R_k$ можно определить покомпонентным сложением и умножением соотв. упор. k-ок.

Если A – (ассоц.) комм. алгебра с 1, то понятия подалгебры, идеала, фактор-алгебры, гом. зма аналогичны, см. также зам. 1 в § 9.2 из [ВШ] о том, что идеал алгебры с 1 = идеал кольца этой алгебры.

Модуль M над кольцом R (R-модуль) – это абелева группа с операцией умножения на эл-ты из R, удовл. сл. усл:

1) $a(x+y) = ax + ay$ $\quad \forall a,b \in R,\ x,y \in M$

2) $(a+b)x = ax + bx$ $\quad$ 3) $(ab)x = a(bx)$ $\quad$ 4) $1 \cdot x = x$

Примеры: 1) $V / \mathbb{F}$ – в.п. над $\mathbb{F}$ – $\mathbb{F}$-модуль

2) любая аб. группа M – $\mathbb{Z}$-модуль

3) $\forall$ кольца R $\quad R^+$ – R-модуль.

Понятие подмодуля

$I \trianglelefteq R \iff I$ – R-подмодуль в R^+.

Фактор-модуль, гом-зм модулей, прямая сумма ....

$\operatorname{Ann} M = \{ a \in R \mid ax = 0 \ \forall x \in R \}$.

Модуль M наз-ся точным, если $\operatorname{Ann} M = 0$, т.е.
$\forall a \in R \ \exists x \in M : ax \neq 0$.

Пусть $S \subseteq R$. $\langle S \rangle_{\text{мод}} = \{s_1 + \dots + s_n \mid s_i \in S\}$ – множество, порожденное S

$(S) = \langle S \rangle_{\text{идеал}} = \{a_1 x_1 + \dots + a_m x_m \mid a_i \in R, x_i \in S, m \in \mathbb{N}\} =$

$= \bigcap I$ – идеал, порожденный множеством S.
$S \subseteq I \trianglelefteq R$

Идеал, который порожд. конечным мн-вом S,
наз-ся конечно порожденным (кратко К.п.)

Идеал, кот. порожд. 1 эл-том, наз-ся главным.

Аналогично для алгебр и модулей, но 1-пор. модуль – циклический

Кольцо Нётерово, если в нем. любое из сл. экв. условий:

1) любой идеал К.п.

2) не существует беск. строго возр. цепочки идеалов

То же для модулей с заменой идеала на подмодуль.

Факты о нётеровых кольцах и модулях:

1) R – нёт. кольцо, $I \trianglelefteq R \Rightarrow R/I$ нётеров (–/– модуль)

2) R – нёт. кольцо, M – вп. R-модуль, $N \leq M \Rightarrow N$ – к.п.

3) (т. Гильберта) R – нёт. $\Rightarrow R[x]$ – нётерово
В частности $F[x_1 .. x_n]$ – нётерово $\forall$ и $\leftarrow \exists$.

2. Области целостности, делимость, факториальность

Эл-т $a \neq 0$ кольца R – делитель нуля, если $\exists b \in R : ab = 0$.

Кольцо R – область целостности, если в нём нет дел. нуля

Идеал $I \trianglelefteq R$ – простой, если R/I – область целостности.

Уп. $I \trianglelefteq R$. Если I – макс., то I – простой.

Упр 2 Привести пример того, что обратное неверно.

Пусть R – область целостности, $a, b \in R$.

$a \mid b$ (a делит b), если $\exists c \in R : ac = b$

$a \sim b$ (a и b ассоциированы), если $a \mid b$ и $b \mid a$

Утв. 1 – отн-е частич. порядка, $\sim$ – отн-е экв-сти.

Эл-т $a \in R^*$ (обратим) $\Leftrightarrow a \mid 1$, т.к. $\exists c \in R \; ac = 1$.

Упр 3 $a \sim b \Leftrightarrow \exists c \in R^* : a = cb$.

Опр 1 Необр. эл-т $a \neq 0$ неприводим, если $a = bc \Rightarrow$ либо b, либо c обратим.

Опр 2 Необр эл-т $a \neq 0$ прост, если $a \mid bc \Rightarrow a \mid b$ или $a \mid c$

Зам. Отличается от §9.7 в [ВИН].

В $\mathbb{Z}$ неприв = прост!

Лемма 1 R – обл. цел. сн., a – прост $\Rightarrow a$ неприводим

Д-во: $a = bc$ для $b, c \in R$. Т.к. a прост, то $a \mid b$ или $a \mid c$. Пусть $a \mid b \Rightarrow \exists d: b = ad \Rightarrow$

$\Rightarrow a = adc \Rightarrow a(1 - dc) = 0 \Rightarrow 1 = dc$ (R – цел. сн.)

$\Rightarrow c$ обратим $\Rightarrow a$ неприводим.

Зам. Обратное неверно, как мы увидим позже.

Язык идеалов: $a \mid b \Leftrightarrow (a) \supseteq (b)$ | $2 \mid 4 \Leftrightarrow 2\mathbb{Z} \supseteq 4\mathbb{Z}$

$a \sim b \Leftrightarrow (a) = (b)$, т.е. a прост $\Leftrightarrow (a)$ – простой идеал.

Лемма 2 R – нётерова обл. цел. сн. $\Rightarrow$ канонич. разл.

Необр. т.е. представим в виде пр-я неприводимых.

Идея Д-то аналогично 2, используя язык идеалов.

Опр 3 Обл. кольцо R наз-ся факториальным кольцом, если в нём каждый необр. элемент представим в виде пр. $\neq$ необр. эл-тов и это представление единств. с точностью до перестановки сомн-лей и умн-ия на обр. эл-т. (до ассоц).

Теорема 1 Обл. ц.о. кольцо R, допуск. разложение в необр., факториальное $\Leftrightarrow$ любой необр. эл-т простой

Δ-во: $\Rightarrow$) p - необр. эл-т. Пусть, что $p \mid ab$, т.е. $pc = ab$. Разложим не необр. a, b, c. Имеем $p u_1 p_1 \dots p_k = u_2 p_1 \dots p_e u_3 q_1 \dots q_m$. Из ФСИ $\Rightarrow p \sim p_i$ или $p \sim q_j$

$\Rightarrow p \mid a$ или $p \mid b$

$\Leftarrow$) пусть $u_1 p_1 \dots p_k = u_2 q_1 \dots q_t$, где u_1, u_2 – обр.

$p_1 \dots p_k$ и $q_1 \dots q_t$ – неприв. Тогда в силу простоты p_1

$\exists i: q_i = u p_1$. „Сокращая" на p_1 получаем по инд. единств. разложения. ▭

(ОГИ)

Область целостности R наз-ся областью главных идеалов если любой идеал – главный ($\forall I \trianglelefteq R\ \exists a \in R: I = (a)$)

<u>Зам.</u> R – ОГИ $\Rightarrow$ R/I – ОГИ, хотя все идеалы снова главные, но целостность может нарушиться.

В ОГИ определён НОД$(x,y) = d$, поскольку идеал $(x,y) = \{ax + by\} = (d)$ – главный, т.е. порожд. одним эл-том.

В частности, x и y вз. просты, если $(x,y) = (1) = R$.

Предл 1 Пусть R – ОГУ, $u, v \in R$ взаимно просты. Тогда
$R/(uv) \cong R/(u) + R/(v)$.

Предл 2 R – ОГУ $\Rightarrow$ R факториально.

Упр 5. Д-ть предл. 1 и 2.

Т. 2 Если кольцо R факториально, то $R[x]$ тоже

Следствие Для поля $\mathbb{F}$ кольцо $\mathbb{F}[x_1, \dots x_n]$ факториально

Д-во: Исп-ем индукцию по лемме Гаусса ($R = \mathbb{Z}$ и $Q = \mathbb{Q}$)
если неприв. из $R[x]$ разл. в пр-е мн-тов
меньшей степени в $Q[x]$, где $Q = Q(R)$ –
поле частных кольца R, то тоже самое можно
сделать и в $R[x]$. См [ВИК, т. 9.7.4].

О расш. полей Вн значение из теории Галуа, см. [ВИН, §9.5]

Кольцо B - расширение кольца A, если $A \subseteq B$.
Если $u_1, \dots u_n \in B$, то $A[u_1, \dots u_n]$ - все те, эл-ты кольца B, которые могут быть представлены в виде $f(u_1, \dots u_n)$, где f - мн-н с коэф-ми из A.
B - к.и. над A, если $\exists u_1, \dots u_n \in B$: $B = A[u_1, \dots u_n]$.

Пример $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

Упр 6* Кольцо $\mathbb{Z}[\sqrt{-5}]$ нётерово, но не факториальное

Указ: Показать, что эл-т 2 из $\mathbb{Z}[\sqrt{-5}]$ неприводим, но не прост: $2 \nmid 1 \pm \sqrt{-5}$ но $2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$.
и Вост. теорема 1.