Экзамен по алгебре

Швецова Анна по конспектам от Саютина Дмитрия

13 января 2017 г.

Содержание

1. Билет 1 **1**

1.1 Определения и основные понятия 1

1.2 Свойства колец 1

1.3 Гомоморфизм колец 2

1.4 Подкольца и идеалы 3

2. Билет 2 **5**

3. Билет 3 **7**

4. Билет 4 **8**

5. Билет 5 **10**

6. Билет 6 **12**

7. Билет 7 **14**

8. Билет 8 **16**

9. Билет 9 **18**

10. Билет 10 **19**

11. Билет 11 **20**

1. Билет 1

1.1. Определения и основные понятия

***Определение* 1.1.** Множество R с операциями $+, \cdot$ на нём называется кольцом, если:

1. $(R, +)$ — абелева группа.
2. $\forall x,\ y,\ z \in R$: $\begin{matrix}(x+y)z = xz + yz \\ x(y+z) = xy + xz\end{matrix}$ (дистрибутивность)

***Определение* 1.2.** Кольцо называется ассоциативным, если $*$ — ассоциативна $(x(yz) = (xy)z)$.

***Определение* 1.3.** Кольцо называется коммутативным, если $*$ — коммутативна $(xy = yx)$.

***Определение* 1.4.** Кольцо называется кольцом с единицей, если $\exists 1 \colon x \cdot 1 = 1 \cdot x = x\ \forall x \in R$.

***Определение* 1.5.** Ассоциативное кольцо с единицей, причём $1 \neq 0$, в котором всякий ненулевой элемент обратим [по умножению] называется телом.

***Определение* 1.6.** Коммутативное тело называется полем.

Пример.
$2\mathbb{Z}$ —коммутативное, ассоциативное кольцо без 1
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/n\mathbb{Z}$
$R[x]$ — кольцо многочленов с коэффициентами из R
$R[[x]] = \{\sum\limits_{i=0}^{\infty} a_i x^i \mid a_i \in R\}$ — кольцо формальных степенных рядов.

1.2. Свойства колец

Лемма. Пусть R - кольцо (ассоциативное), $r \in R$, тогда:

1. r * 0 = 0 * r = 0
2. Если R - кольцо с единицей, то $(-1) * r = -r$, где $(-x)$ означает обратный элемент по сложению.
3. Если $|R| \neq 1$, то $0 \neq 1$.

Доказательство.

1. - $r + 0 = r = 0 + r$.
   - $r(r+0) = r^2$
   - $r^2 + r * 0 = r^2$
   - $r * 0 = 0$.
   - Аналогично доказывается правое равенство.
2. Пользуемся дистрибутивностью кольца:
   $r * 0 = 0 \Rightarrow r(-1+1) = 0 \Rightarrow .\ (-1)r + 1 * r = 0 \Rightarrow (-1)r + r = 0 \Rightarrow (-1) * r = (-r)$

3. Пусть $0 = 1$. Тогда $\forall r \in R\colon r = 1 * r = 0 * r = 0 \implies R = \{0\} \implies |R| = 1$. □

***Определение* 1.7.** Пусть R — коммутативное кольцо. Элемент $r \in R\backslash\{0\}$ называется делителем нуля, если $\exists s \in R \setminus \{0\}\colon rs = 0$.

***Определение* 1.8.** Пусть R — коммутативное кольцо. Элемент $r \in R \setminus \{0\}$ называется нильпотентным, если $\exists n \in \mathbb{N}\colon r^n = 0$

Замечание 1. В $\mathbb{Z}/n\mathbb{Z}$ есть делители нуля $\iff$ n – составное.

- Если $n = ml$ $(m, l \geqslant 2)$, то и m и l - делители нуля.
- Если есть делители нуля, то $\exists m, l \geqslant 2,\ ml \vdots n$, что невозможно.

Так что в качестве примера можно привести какое-нибудь составное число и его делитель.

Замечание 2. В $\mathbb{Z}/n\mathbb{Z}$ нильпотенты $\iff$ n делится на какой-то квадрат.

TODO: Нужно больше примеров

***Определение* 1.9.** Коммутативное ассоциативное кольцо с 1 без делителей нуля называется областью целостности (целостным кольцом).

1.3. Гомоморфизм колец

***Определение* 1.10.** $f\colon A \to B$ называется гомоморфизмом колец, если:

- A, B — кольца.
- $\forall a,\ b \in A\colon f(a + b) = f(a) + f(b)$.
- $\forall a,\ b \in A\colon f(ab) = f(a)f(b)$.

***Определение* 1.11.** $\operatorname{Ker} f = f^{-1}(0) = \{x \in A \mid f(x) = 0\}$

***Определение* 1.12.** $\operatorname{Im} f = \{f(x) \mid x \in A\}$.

Замечание. Если $f\colon A \to B$ — гомоморфизм колец, то:

1. $f(0_A) = 0_B$
2. $f(-r) = -f(r)$
3. Если $f(a) = b$, то $f^{-1}(b) = a + \operatorname{Ker} f$
4. f — инъективна $\iff$ $\operatorname{Ker} f = \{0\}$

Доказательство.

1. $f(0_A) = f(0_A * 0_A) = f(0_A) * f(0_A) \Rightarrow f(0_A) = 0_B$
2. $0_B = f(0_A) = f(-r + r) = f(-r) + f(r) \Rightarrow f(-r) = -f(r)$
3. Если $f(a) = b$, то $f^{-1}(b) = a + \operatorname{Ker} f$
   Докажем вложенность в обе стороны.
   $a + \operatorname{Ker} f \subset f^{-1}(b)$ т.к. $\forall x \in \operatorname{Ker} f f(a + x) = f(a) + f(x) = f(a) + 0 = f(a) = b$
   В другую сторону: пусть есть элемент $t \notin a + \operatorname{Ker} f\ :\ f(t) = b$, тогда $0 = f(t) - f(a) = f(t - a) \Rightarrow t - a \in \operatorname{Ker} f \Rightarrow t - a + a \in a + \operatorname{Ker} f \Rightarrow t \in a + \operatorname{Ker} f$ Протворечие
4. f — инъективна $\Rightarrow \forall x \in B\ |f^{-1}(x)| \leqslant 1 \Rightarrow |\operatorname{Ker} f| = |f^{-1}(0)| \leqslant 1$ Но там есть хотя бы 0, значит, строго 1. В обратную строну очевидно. Если ядро нетривиально, значит, хотя бы прообраз нуля ломает инъективность.

□

Замечание. Единица не всегда сохраняется, даже если она есть во втором кольце.

Пример. A — абелева группа, есть $+$, 0. $x, y \in A$: $x \cdot y := 0$.

***Определение* 1.13.** Гомоморфизм нулевой, если он переводит все элементы в 0.

Утверждение 1.1. Если $f\colon A \to B$ ненулевой гомоморфизм колец. A — кольцо (ассоциативное, коммутативное) с 1. B — область целостности, то $f(1_A) = 1_B$.

Доказательство. $f(1_A) = f(1_A * 1_A) = f(1_A) * f(1_A)$

$f(1_A) - f(1_A) * f(1_A) = 0_B$

$f(1_A)(1_B - f(1_A)) = 0_B$.

Так как B — область целостности, то $f(1_A) = 0$ или $f(1_A) = 1_B$.

Если $f(1_A) = 0_B$, то $\forall a \in A$: $f(a) = f(1 * a) = f(1)\, f(a) = 0\, f(a) = 0 \implies f$ — нулевой.

Следовательно $f(1_A) = 1_B$. □

Замечание. Далее гомоморфизм колец с единицей означает гомоморфизм колец, обладающий свойством выше ($f(1_A) = 1_B$).

Лемма. Если $f\colon A \to B$ — гомоморфизм колец с единицей, то $\forall x \in A^*$: $f(a^{-1}) = f(a)^{-1}$

Доказательство.
Если a обратим, то $aa^{-1} = 1$. Тогда $1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1}) \Rightarrow f(a)^{-1} = f(a^{-1})$ □

Лемма. Если $f\colon A \to B$ — гомоморфизм колец, то

$\operatorname{Im} f$ — подкольцо B.

$\operatorname{Ker} f$ — двусторонний идеал A.

Доказательство. Оставлено в качестве упражнения. □

1.4. Подкольца и идеалы

***Определение* 1.14.** Непустое подмножество кольца R называется подкольцом, если

- $\forall a, b \in A$: $a + b$, $-a$, $ab \in A$

***Определение* 1.15.** Аддитивная подгруппа $I \leqslant R^+$ называется:

- Левым идеалом, если $\forall r \in R, \forall s \in I$: $rs \in I$ (иначе говоря, $RI \subseteq I$)
- Правым идеалом, если $\forall r \in R, \forall s \in I$: $sr \in I$ (иначе говоря, $IR \subseteq I$).
- Двусторонним идеалом, если она и левый и правый идеал.

// Все примеры живут в конспекте так как в билете они не требуются. Итак он очень большой

***Определение* 1.16.** R — кольцо, $X \subseteq R$. Идеалом (левым, правым, двусторонним), порождённым подмножеством X называется наименьший по включению идеал (левый, правый, двусторонний), содержащий X.

Упражнение: пересечение всех идеалов, содержащих данное множество X является идеалом, порождённым множеством X.

Доказательство.

Во-первых, пересечение идеалов – идеал. (Идеалы это подгруппы, пересечение подгрупп = подгруппа. Соблюдение свойства идеала проверяется так: возьмем элемент из пересечения, домножим на любое r. Полученный элемент лежал в обоих идеалах, значит и в пересечении тоже. Успех)
Во вторых, мы получим не меньше чем нужный идеал. Пусть не так. Тогда какие-то 2 идеала пересеклись и мы получили меньше чем нужный идеал. Но в результате пересечения мы получили идеал и он также содержал множество . Значит, наименьший идеал не наименьший. Противоречие.
В-третьих, мы получим не больше, так как в пересечении уже лежит искомый идеал. □

Замечание. Для правых идеалов:

$$\bigcap_{\substack{I \supseteq X \\ \text{I} - \text{идеал R}}} I = \sum_{x \in X} xR$$

***Определение* 1.17.**

- (X) — идеал, порождённый множеством X, в зависимости от ситуации левый, правый или двусторонний.
- (a) — идеал, порождённый элементом a, где $a \in R$, в зависимости от ситуации левый, правый или двусторонний.
- Идеал, порождённый одним элементом называется *Главным идеалом.*

Замечание. Для левых идеалов $(a) = Ra$.

Лемма. Подкольцо, порождённое множеством X, то есть наименьшее подкольцо, содержащее это множество, состоит из всех сумм из элементов $\pm x_1 x_2 x_3 \dots x_n$, где $x_i \in X$

Доказательство. □

2. Билет 2

***Определение* 2.1.** Пусть R — кольцо с 1, введём *канонический гомоморфизм* $\phi : \mathbb{Z} \to R$:

$$\phi(n) = \begin{cases} 0 & n = 0 \\ \underbrace{1_R + 1_R + \ldots + 1_R}_{n \text{ раз}} & n > 0 \\ -\phi(-n) & n < 0 \end{cases}$$

Действительно является гомоморфизмом (следствие дистрибутивности).

***Определение* 2.2.** Если канонический гомоморфизм ϕ — инъективен ($\operatorname{Ker}\phi = \{0\}$), то характеристика ноль ($\operatorname{Char} R := 0$)

Иначе ядро нетривиально. Но в $\mathbb{Z}$ любое нетривиальное ядро имеет вид $n\mathbb{Z}$ (для некоторого $n \geqslant 1$, ибо ядро – это подгруппа), такое n и называется характеристикой кольца R ($\operatorname{Char} R = n$).

Любой идеал I по определению является подгруппой аддитивной подгруппы кольца и задаёт разбиение кольца на смежные классы или классы вычетов по модулю I, о чём пойдёт речь дальше.

***Определение* 2.3.** a и b сравнимы по модулю I ($a \equiv b \mod I$), если $a - b = a + (-b) \in I$,

Где $a, b \in R$, I — идеал R (левый, правый, или двусторонний).

Лемма. Если I — двусторонний идеал, $a \equiv a' \pmod I$, $b \equiv b' \pmod I$, то

1. $a + b \equiv a + b' \equiv a' + b' \pmod I$.
2. $ab \equiv ab' \equiv a'b' \pmod I$

Доказательство.

1. $a + b - (a + b') = b - b' \in I \Rightarrow a + b \equiv a + b'$. Остальное аналогично
2. $ab - ab' = a(b - b') \in I$. (так как $b - b' \in I$, и I — идеал) □

***Определение* 2.4.** Пусть I — двусторонний идеал R.

- Фактор-кольцом по I называется множество смежных классов в сравнимости по модулю.
- Зададим сложение: R/I: $(r_1 + I) + (r_2 + I) = r_1 + r_2 + I$.
- Зададим умножение: R/I: $(r_1 + I)(r_2 + I) = r_1 r_2 + I$.
- Проверим дистрибутивность слева: $(r_1+I)(r_2+I+r_3+I) = (r_1+I)(r_2+r_3+I) = r_1r_2+r_1r_3+I$.
- Дистрибутивность справа. $(r_2 + I + r_3 + I)(r_1 + I) = (r_2 + r_3 + I)(r_1 + I) = r_2r_1 + r_3r_1 + I$.
- **Упражнение:** Доказать корректность (независимость результата сложения и умножения от выбора представителя). План доказательства: Взять 2 класса вычетов, из каждого взять по 2 элемента. Показать (сравнимостью), что неважно, какой из элементов из одного класса мы будем брать, мы всё равно попадем в один класс.

Пример 1. $\mathbb{Z}/_{n\mathbb{Z}}$ теперь является не только фактор-группой, но и фактор-кольцом.

Пример 2. $K[x]/_{(f(x))}$
K — поле, $f \in K[x]$.

3. Билет 3

Теорема 3.1 (Теорема о гомоморфизме)**.** Пусть f — гомоморфизм колец с 1. Тогда $A/_{\operatorname{Ker} f} \simeq \operatorname{Im} f$.

Доказательство. Из теоремы о гомоморфизме групп у нас есть: $\phi\colon A/_{\operatorname{Ker} f} \to \operatorname{Im} f$

Нужно показать гомоморфизм умножения: $\phi(ab) = \phi(a)\,\phi(b)$.

Что оставляется как упражнение читателю. □

***Определение* 3.1.** Пусть R_1, R_2 — кольца.

Определим $R_1 \oplus R_2 = \{(r_1, r_2)\}$, кольцо.

Зададим сложение: $(a,\, b) + (c,\, d) = (a + b,\, c + d)$

Зададим умножение: $(a,\, b) * (c,\, d) = (ab, cd)$.

Замечание. Аналогично вводится прямая сумма для большего числа слагаемых.

Замечание. Иногда преподаватели алгебры применяют обозначение $\times$ вместо $\oplus$ (смотрите далее).

Замечание. В данной конструкции много делителей нуля.

Действительно, любой элемент вида $(r,\, 0)$ или $(0,\, r)$ (в случае двух колец) является делителем нуля.

4. Билет 4

Здесь и далее в главе R означает коммутативное кольцо, а I, J – его идеалы.

Лемма. $I \cap J$ идеал.

Доказательство. Доказано выше где-то здесь. (1.16). □

***Определение* 4.1.** Определим $I + J = \{a + b \mid a \in I, b \in J\}$ как все возможные суммы.

Замечание. $I + J$ является идеалом, так как:

- $I + J$ несомненно образует подгруппу аддитивной группы кольца.
- $\forall a \in I, b \in J\ a + b \in I + J$. $\forall r \in R\ r(a + b) = ra + rb, ra \in I, rb \in J \Rightarrow ra + rb \in I + J$

Замечание. $I + J$ наименьший идеал содержащий и I и J. Иначе говоря, $I + J = (I \cup J)$, то есть идеал порождённый объединением.

***Определение* 4.2.** Произведение идеалов $IJ = (\{ab \mid a \in I, b \in J\})$ — это идеал порождённый всеми попарными произведениями.

Замечание. $IJ \neq \{ab \mid a \in I, b \in J\}$, так как полученное множество идеалом не является.

$$IJ = \{\sum a_i b_i \mid a_i \in I, b_i \in J\}.(ra)b, ra \in I$$

.

***Определение* 4.3.** Идеалы I, J называются взаимно простыми, если $I + J = R$.

Здесь и далее все кольца имеют единицу.

Лемма. Если I, J взаимно просты, то $IJ = I \cap J$

Доказательство.

- $IJ \subseteq I \cap J$.

  $\forall r \in IJ$: $r = \sum\limits_{i=1}^{N} a_i b_i$, где $a_i b_i \in I \cap J$ но это значит, что и их сумма лежит в пересечении. Мне тут было неочевидно, почему бы вдруг $a_i b_i \in I \cup J$. Так вот из определения идеала. $a_i \in I \Rightarrow a_i b_i \in I$, (если домножаемся на любой элемент и в том числе на b_i – попадаем в то же кольцо). Аналогично для J (помним про наличие коммутативности).

- $IJ \supseteq I \cap J$.

  I и J — взаимно просты $\implies$ $I + J = R \ni 1$.

  $\implies$ $\exists a \in I, b \in J$ такие что $a + b = 1$ (см 4.1)

  $\forall x \in I \cap J$: $x = x * 1 = x * (a + b) = xa + xb$.

  $xa \in (I \cap J)I$, $xb \in (I \cap J)J$. (Ну понятно для обоих произведений. $I \cup J$ – это меньше, и чем I, и чем J и одновременно их подмножества)

  $xa + xb \in IJ$. □

Замечание. Обратите внимание, что $IJ \subseteq I \cap J$ для всех идеалов I, J, так как в первой части леммы не пользуемся тем, что I, J — взаимно простые.

Теорема 4.1. Пусть R — коммутативное ассоциативное кольцо с 1, а I, J — взаимно простые идеалы.

Тогда $R/IJ \cong R/I \oplus R/J$

Замечание. В частном случае мы уже знаем это утверждение, если $(n, m) = 1$, то:

$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.

Доказательство. $f\colon R \to R/I \oplus R/J$.

Сопоставим объекту два его класса по модулям I, J: $f(r) := (r \mod I, r \mod J)$, где $r \mod I = r + I$.

Каждая проекция является гомоморфизмом, значит f тоже гомоморфизм.

$\operatorname{Ker} f = \{r \in R \mid r \in I, r \in J\} = I \cap J = IJ$

По теореме о гомоморфизме колец (см 3.1) получаем требуемое. Осталось доказать, что полученное – эпиморфизм. Т.к. I и J взаимно простые, то $\exists a \in I, b \in J : \ a + b = 1$, тогда $\forall x, y \in R \ xb + ya$ – прообраз $(x + I, y + J)$.

□

Лемма. Пусть R — ассоциативное коммутативное кольцо с 1.

Если идеал I взаимно прост с каждым из идеалов $J_1, \ldots, J_k$, то I взаимно прост с их произведением $J_1 J_2 \ldots J_k$

Доказательство. $R = I + J_1 = I + J_1 R = I + J_1(I + J_2) = I + J_1 I + J_1 J_2 \subset I + J_1 J_2$

И, видимо, так как $I + J_1 J_2 \subset R$ как идеал кольца, то в последнем переходе можно поставить равенство.

И так далее до любого конечного k:

$R = I + J_1 J_2 = I + J_1 J_2 R = I + J_1 J_2 (I + J_3) = \ldots = I + J_1 J_2 J_3$

Здесь мы пользуемся определением идеала (1.15), суммы идеалов (4.1), определением взаимной простоты (4.3). □

5. Билет 5

Теорема 5.1 (Китайская Теорема об Остатках)**.** Пусть $I_1, I_2, \ldots, I_n$ — попарно взаимнопростые идеалы в R.

Тогда $R/_{I_1 I_2 \ldots I_n} \cong R/_{I_1} \oplus R/_{I_2} \oplus \ldots \oplus R/_{I_n}$

Доказательство. Доказательство теоремы несложно получить из индукции, предыдущей леммы и теоремы 4.1.

Есть такое. Если неочевидно, то индукция такая:
База: тривиальный фактор. Тогда всё изоморфно само себе, говорить не о чем.
Переход: отщепим любой нетривиальный нужный нам идеал I, взаимнопростой с оставшимися. По теореме, получим изоморфизм по факторам I и $J_1 J2_2 \ldots$. Из леммы выше знаем, что если I взаимнопросто с оставшимися идеалами, то I и $J_1 J_2 \ldots$ тоже взаимнопросты. Применяем индукцию и радуемся □

Замечание. Если R — кольцо целых чисел, то теорему можно сформулировать следующим образом:

Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимнопростые целые числа, $n := m_1 m_2 ... m_k$.

Тогда $\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}/_{m_1\mathbb{Z}} \oplus \ldots \oplus \mathbb{Z}/_{m_k\mathbb{Z}}$

Теорема 5.2 (Решение систем сравнений в целых числах)**.**
Для любого набора остатков $r_1 \ldots r_k$ $\exists x \in \mathbb{Z}$, такой что:

$$\begin{cases} x \equiv r_1 \mod m_1 \\ x \equiv r_2 \mod m_2 \\ \ldots \\ x \equiv r_k \mod m_k \end{cases} \qquad (m_i, m_j) = 1 \text{ для } i \neq j.$$

Причём если x и y являются решениями этой системы, то $x \equiv y \pmod n$.

Доказательство.

Определим $n := m_1 m_2 \ldots m_k$, $n_i := n/m_i$.

Так как m_i и n_i взаимнопросты, то $\exists x_i, y_i \in \mathbb{Z}$: $m_i x_i + n_i y_i = r_i$

С практической точки зрения их можно найти, например, с помощью алгоритма Евклида.

Заметим, что

- $n_i y_i \equiv r_i \pmod{m_i}$
- $n_i y_i \equiv 0 \pmod{m_j}$ для $j \neq i$

Первое следует из $m_i x_i + n_i y_i = r_i$, второе из $n_i = n/m_i = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$.

Определим $x := \sum_{i=1}^{k} n_i y_i$.

Тогда $\forall i$: $x \equiv n_i y_i \equiv r_i \pmod{m_i}$.

Вторая часть доказательства проще:

Пусть x — решение системы.

- Если y — решение, то $y - x \vdots m_i$, значит $y - x \vdots n$.

- Если y таков, что $y - x \vdots n$, то $y = x + nt$, подставляем в систему, nt сокращается.

□

6. Билет 6

***Определение* 6.1.** Элемент b делит элемент a (записывается как $b \mid a$), если $a = bc$ для некоторого $c \in R$.

Утверждение 6.1.

- $b|a \iff a \in bR \iff aR \subseteq bR$
- $a \in R^* \iff aR = R$

Доказательство.

- $a = bc\ c \in R \Rightarrow a \in bR \Rightarrow aR = b(cR) \subseteq bR$ так как $cR \subset R$
  И в обратную: $aR \subseteq bR \Rightarrow \forall x \in R \exists y \in R:\ ax = by \Rightarrow a * 1 = a \in bR \Rightarrow \exists c : a = bc \Rightarrow b|a$
- $\forall x \in R a^{-1}x \in R \Rightarrow aa^{-1}x = x \in aR$
  $\forall x \in R \exists y \in R : x = ay \Rightarrow \exists y : 1 = ay \Rightarrow a$ – обратим.

□

***Определение* 6.2.** Пусть I — идеал, тогда I простой, если $\forall a, b \in R$: $ab \in I \implies a \in I \vee b \in I$.

***Определение* 6.3.** I — максимальный, если для любого идеала J: $I \subsetneq J \subset R \implies J = R$.

Лемма. Пусть I — идеал R, тогда $\exists J$ — идеал, $I \subseteq J \subseteq R$ и J максимальный.

Доказательство. Рассмотрим множество $X = \{K \mid K$ — идеал в$R, K \supseteq I, K \neq R\}$, введём на нём частичный порядок включения ($\subseteq$).

Покажем, что любое линейно упорядоченное подмножество X имеет верхнюю грань.

Пусть $\{L_i\}$ — произвольное линейно упорядоченное подмножество, $L := \bigcup L_i$.

Рассмотрим произвольные $a, b \in L$, тогда $a \in L_i, b \in L_j$ (для некоторых i, j).

Но множество линейно упорядоченно, значит одно лежит в другом (совпадение тоже допускается), без потери общности давайте считать, что $L_i \subseteq L_j$.

Следовательно $a, b \in L_j \implies a - b \in L_j \subseteq L$.

Также $\forall r \in R$: $ra \in L_j \subseteq L$.

Итого мы получаем по определению (1.15), что L — идеал. Значит любое линейное упорядоченное подмножество X имеет верхнюю грань, значит (по лемме Цорна) в множестве X есть максимальный элемент.

Соответственно этот максимальный элемент и является максимальным идеалом. □

Замечание. R — область целостности $\iff \{0\}$ — простой идеал.

Область целостности $\iff ab = 0 \implies a = 0 \vee b = 0$.

Идеал простой $\iff ab \in \{0\} \implies a \in \{0\} \vee b \in \{0\}$.

Утверждение 6.2. Пусть R — коммутативное ассоциативное кольцо с 1, I — идеал в R, тогда:

1. I — простой $\iff R/_I$ — область целостности.
2. I — максимальный $\iff R/_I$ — поле.
3. Если I — максимальный, то I — простой.

Доказательство.

“$\to$”. (!) в $R/_I$ нет делителей нуля.

$(a+I)(b+I) = I \implies a \in I \vee b \in I$.

$(a+I)(b+I) = ab + I$

“$\leftarrow$” $(a+I)(b+I) = I \Rightarrow a + I \in I \vee b + I = I \Rightarrow a \in I \vee b \in I$

Тут было написано что-то не очень похожее на правду. Смотрите следствие 9 в конспекте лектора □

Далее R область целостности

Утверждение 6.3. В кольце главных идеалов R любой ненулевой простой идеал I является максимальным

Доказательство. $I = pR$, пусть $I \subsetneq J \subseteq R$, J — идеал.

R — КГИ $\implies J = qR \;\; pR \subseteq qR \subseteq R$

$p = qr$, pR — простой $\implies (q \in pR \implies pR = qR) \vee (r \in pR \implies r = ps)$.

$p = qr = qspp(1 - qs) = 0 \implies q \in R^* \iff qR = R$.

Если не получилось, страница 32 конспекта лектора, там даже нет слова «очевидно» □

7. Билет 7

Пусть R — область целостности.

***Определение* 7.1.** $a, b \in R$, a и b ассоциированные, если $aR = bR$.

(или, эквивалентно, $aR \subseteq bR$, $bR \subseteq aR \iff a|b, b|a$).

Пример 1. В $\mathbb{Z}$ n и m ассоциированы, если $n = m$ или $n = -m$.

Пример 2. В $K[x]$ (где K — поле) f и g ассоциированы, если $f(x) = cg(x)$, $c \in K[x] \setminus \{0\}$.

Пусть $a \sim b$, если a ассоциирован с b.

***Определение* 7.2.** Пусть $a \in R \setminus R^*$. Элемент a неприводим, если $a = bc \implies a \sim b \vee a \sim c$.

***Определение* 7.3.** Пусть $p \in R \setminus R^*$. Элемент p называется простым, если $p \mid ab \Rightarrow p \mid a \vee p \mid b$.

Замечание. Ассоциированость является отношением эквивалентности.

Лемма. Пусть $a, b \in R \setminus \{0\}$, тогда:

1. $a \sim b \iff a = b\varepsilon$, где $\varepsilon \in R^*$.
2. a — неприводим $\iff (a = cd \implies c \in R^* \vee d \in R^*)$.

Доказательство.

1. - “$\implies$”

     $a \sim b \iff \begin{cases} b|a \implies a = b\varepsilon \implies a = a\delta\varepsilon \implies a(1 - \delta\varepsilon) = 0 \implies \delta\varepsilon = 1 \implies \varepsilon \in R^* \\ a|b \implies b = a\delta \end{cases}$

     Пользуемся тем, что мы в области целостности, а также тем, что $a \neq 0$.
   - “$\impliedby$”

     a и b ассоциированные $\iff a \mid b$, $b \mid a$.

     $a = b\varepsilon$, $b = a\varepsilon^{-1}$ (пользуемся коммутативностью, обратимостью ε).

     После этого делимость очевидна по определению (см 6.1)
2. $a = bc \implies (a \sim b \vee a \sim c)$

   Пусть б.п.о. $a \sim b \implies a = b\varepsilon, \varepsilon \in R^* \implies b\varepsilon = bc \implies b(\varepsilon - c) = 0 \implies c = \varepsilon$. $a = bc$

□

***Определение* 7.4.** R — область целостности. R — факториально, если любой элемент единственным образом раскладывается в произведение неприводимых.

Единственность вплоть до порядка и ассоциированости:

Если $\varepsilon p_1 p_2 \dots p_n \sim \Theta q_1 q_2 \dots q_m$ (где p_i, q_j неприводимы, $\varepsilon, \Theta \in R^*$), то $n = m$ и $\exists \sigma \in S_n \colon p_i \sim q_{\sigma(i)}$

Теорема 7.1. Если R — кольцо главных идеалов, то R факториально.

Доказательство состоит из нескольких лемм:

Лемма (1). R — кольцо главных идеалов, $a, c \in R, c$ — неприводим, $\neg c|a \implies aR + cR = R$

Доказательство. R — кольцо главных идеалов $\implies aR + cR = bR \implies c \in bR \implies c = bd$.

Так как c неприводим, то $c \sim b$ или $b \in R^*$.

Но $c \sim b \iff cR = bR$, но тогда $a \in bR = cR$, т.е. $c|a$, но это ложь.

$b \in R^* \iff bR = R$, что мы и хотели. □

Лемма (2)**.** R — кольцо главных идеалов, $a, b, c \in R$, c неприводим.

Тогда $(c|ab \implies c|a \vee c|b)$

Иначе говоря, cR простой: $ab \in cR \implies a \in cR \vee b \in cR$

Доказательство. $c|ab$, пусть $\neg c|a$ и $\neg c|b$.

Тогда по предыдущей лемме $cR + aR = R$ и $cR + bR = R$, из чего по какой-то лемме из китайской теоремы об остатках следует, что cR взаимно прост с $(aR)(bR) = abR$.

Итого: $cR + abR = R$ и $ab \in cR$.

Но $cR + abR = cR$ (так как $c|ab$), следовательно $cR = R$, что возможно $\iff$ обратим.

Но c неприводим, противоречие. □

***Определение* 7.5.** Кольцо R называется нётеровым, если для любой последовательности идеалов I_n в R, такой что $I_1 \leqslant I_2 \leqslant I_3 \leqslant \ldots$, все идеалы начиная с некоторого места совпадают.

Лемма (3)**.** Если R — кольцо главных идеалов, то R нётерево.

Доказательство. Так как R — кольцо главных идеалов, то каждый идеал $I_k = r_k R$ для некоторого r_k.

Докажем, что $I := \bigcup\limits_{i=1}^{\infty} I_i$ идеал:

- $a, b \in I \implies a, b \in I_i \implies a - b \in I_i \implies a - b \in I$
- $a \in I \implies a \in I_i \implies \forall r\colon ra \in I_i \implies \forall r\colon ra \in I$

(Первое условие гарантирует, что I — является подгруппой аддитивной группы кольца, хотя это немного не очевидно сходу. Hint: a может быть равно 0).

Следовательно $I = qR$, для некоторого $q \in R$ (так как мы в кольце главных идеалов).

Следовательно $\exists n\colon q \in I_n = r_n R$ (Если $I = qR$, то q лежит в объединении, значит, q лежит в каком-то идеале начиная с какого-то n)

$q \in I_{n+1} = r_{n+1}R \implies qR \subseteq I_{n+1}$, но $qR \supseteq I_{n+1} \implies qR = I_{n+1}$. □

8. Билет 8

Напомню, что мы доказываем такую теорему:

Если R — кольцо главных идеалов, то R факториально.

Лемма (4)**.** Пусть R — кольцо главных идеалов. Тогда любой ненулевой необратимый элемент раскладывается в произведение неприводимых.

Доказательство. $r \in R \setminus R^*, r \neq 0$.

rR содержится в некотором максимальном идеале M.

$M = p_1R, rR \subseteq p_1R \iff r = p_1r_1, r_1 \in R$

p_1R — max $\implies$ p_1R — простой $\implies$ $(ab \vdots p_1 \implies a \vdots p_1 \vee b \vdots p_1)$

$p_1 = ab \implies a \sim p_1 \vee b \sim p_1$

И из всего этого следует, что p_1 неприводим, т.е.

$r = p_1r_1$, p_1 неприводим.

Если $r_1 \in R^*$, то $r = p_1r_1$ — искомое разложение. Хз.

Если $r_1 \notin R^*$, то $r_1R \neq R$, поэтому $r_1R \subseteq p_2R$ — максимальный. $r = p_1p_2r_2$.

И так далее можно продолжать раскладывать.

Либо $r_k \in R^*$, тогда успех.

$$r_1 = p_2r_2, r_1R \subseteq r_2R \tag{1}$$
$$r_2 = p_3r_3, r_2R \subseteq r_3R \tag{2}$$

$\implies r_1R \subsetneq r_2R \subsetneq r_3R \ldots$, далее всё хорошо по лемме 3. □

Лемма (5)**.** Если:
- R — область целостности.
- $\forall$ неприводимого элемента его идеал прост.
- $\forall$ ненулевого необратимого элемента есть разложение в произведение

То R — факториально.

Доказательство. Достаточно доказать единственность разложения, воспользуемся индукцией по $\min(n, m)$

$n = 0$, ...

Переход: $n > 0 p_n$ — неприводим $\implies$ p_nR — прост.

$\exists l\colon 1 \leqslant l \leqslant m, q_l \in p_nR, q_l \vdots p_n$. Объяснение от меня (возможно, есть проще): $\theta q_1q_2 \ldots q_m = p_n(\epsilon p_1p_2 \ldots p_{n-1}) \in p_nR \Rightarrow \theta \in p_nR \vee q_1q_2 \ldots q_m \in p_nR$. Если из них лежит обратимый, то p_nR – всё кольцо. Короче, $q_1q_2 \ldots q_m \in p_nR$ 100% Теперь $q_1 \in p_nR \vee q_2 \ldots q_m \in p_nR$ и так далее... Приходим к тому, что $\exists q_l \in p_nR$.

a) q_l — неприводим, $q_l = p_n\delta$ (т.к. q_l в кольце), $\delta \in R^* \implies q_l \sim p_n$.

b) Также $\varepsilon p_1 \ldots p_n \sim \Theta q_1 \ldots q_m$

(a), (b) $\implies \varepsilon p_1 \ldots p_{n-1} \sim \Theta q_1 \ldots q_{l-1}q_{l+1} \ldots q_m$.

По предположению индукции $n - 1 = m - 1 \implies n = m$

$\exists$ биекция $t\colon \{1, \ldots, n-1\} \to \{1, \ldots l-1, l+1, \ldots m\}$, $p_i \sim q_{t(i)}$.

$$sigma \in S_n \colon \sigma(i) = \begin{cases} t(i) & i \leqslant n-1 \\ l & i = n \end{cases}$$ □

Замечание. Из всего вышесказанного следует теорема о факториальности кольца главных идеалов.

9. Билет 9

***Определение* 9.1.** Пусть R — область целостности, назовём R евклидовым, если $\exists \nu\colon R\setminus\{0\} \to \mathbb{N}\sqcup\{0\}$:

$\forall a, b \in R\setminus\{0\}$:

1) $\nu(ab) \geqslant \nu(a)$

2) $\exists q, r \in R\colon a = bq + r$ и $r = 0 \vee \nu(r) < \nu(b)$

Функция ν называется евклидовой нормой.

Пример 1. $\mathbb{Z}$, $\nu(x) = |x|$.

Пример 2. K — поле, рассмотрим $K[x]$: $\nu(f) = \deg f$.

Пример 3. $\mathbb{Z}[i] := \mathbb{Z}[x]/_{(x^2+1)},\ \nu(a+bi) = a^2 + b^2$

Пример 4. $\mathbb{Z}[i] := \mathbb{Z}[x]/_{(x^2+x+1)},\ \nu(a+bi) = a^2 + b^2 - ab$

Утверждение 9.1. Евклидовы кольца $\subset$ кольца главных идеалов $\subset$ факториальные $\subset$ области целостности.

Доказательство. Покажем, что R — евклидово кольцо, то R — кольцо главных идеалов.

Рассмотрим произвольный нетривиальный идеал I в R (если $I = \{0\}$, то $I = 0R$)

Рассмотрим элемент $b \in I$ с минимальной нормой: $\nu(b) = \min\limits_{r\in I} \nu(r)$, покажем, что $bR = I$.

Пусть $a \in I$, тогда $\exists q, r\colon a = bq + r$, причём $r = 0 \vee \nu(r) < \nu(b)$.

Но $r = a - bq \in I$, так как $a \in I, bq \in I$.

Так как b имеет минимальную норму, то $r = 0$ или $\nu(r) \geqslant \nu(b)$, следовательно $r = 0$, $a = bq$.

Так как выбрать a можно произвольно, получаем, что идеал I главный $(I = bR)$ □

10. Билет 10

R — область целостности.

***Определение* 10.1.** $d = \gcd(a, b)$, если $d|a$, $d|b$, и из $c|a$, $c|b$, следует $c|d$.

Замечание.

1. $d = gcd(a, b) \iff dR$ — наименьший главный идеал, содержащий и a и b. $(aR + bR)$.
2. gcd Определён с точностью до ассоциативности.

Теорема 10.1.
Пусть R — кольцо главных идеалов.

$a, b \in R$, тогда $\exists x, y \in R$: $ax + by = gcd(a, b)$.

Доказательство. R — кольцо главных идеалов $\implies$
$aR + bR = dR$ и $gcd(a, b) = d \in dR = aR + bR = \{ax + by \mid x, y \in R\}$. □

***Определение* 10.2.** a, b — взаимно простые, если у них нет необратимых общих делителей.

Утверждение 10.2. R — кольцо главных идеалов, $a, b \in R$. Тогда a,b — взаимно простые $\iff$ aR, bR — взаимно простые.

Доказательство. a, b — взаимно простые $\iff$ $1 = gcd(a, b)$ $\iff$ $1 = ax + by$ $\iff$ $R = aR + bR$ $\iff$ aR, bR — взаимно простые. □

***Определение* 10.3.** $a, b \in R, l = \operatorname{lcm}(a, b)$, если $a \mid l$, $b \mid l$, и если $a \mid c, b \mid c \implies l \mid c$.

Замечание. $l = \operatorname{lcm}(a, b) \iff lR$ — наибольший главный идеал, содержащийся в $aR \cap bR$.

Замечание. $a|b \iff bR \subseteq aR$.

Теорема 10.3. a, b — кольцо главных идеалов, $a, b \in R \setminus \{0\}$, тогда $\operatorname{lcm}(a, b) = ab/gcd(a, b)$.

При этом последнее равенство верно с точностью до ассоциированности.

Доказательство. $d = \gcd(a, b)$.

$a = a'd$, $b = b'd$, $a', b' \in R$.

$d = ax + by \implies 1 = a'x + b'y$, более формально:

$d(1 - a'x - b'y) = 0$, но $d \neq 0$ а R — область целостности, следовательно $1 - a'x - b'y = 0$.

$\operatorname{lcm}(a, b)R = aR \cap bR$. (Т.к. все идеалы главные, а мы ищем максимальный из всех вложенных)

$ab/d = a'b'd$.

$c \in aR \cap bR$

$c \in bR, ca' \in ba'R$, $c \in aR, cb' \in ab'R$

$c = c * 1 = ca'x + cb'y \in ba'R + ab'R = a'b'dR$.

$\operatorname{lcm}(a, b)R = aR \cap bR \subseteq a'b'dR = \frac{ab}{d}R$

“$\supseteq$”,

$$a'b'd = ab' \in aR \tag{3}$$

$$a'b'd = ba' \in bR \tag{4}$$

$a'b'd \in aR \cap bR \implies a'b'dR \subseteq aR \cap bR \Rightarrow lcm = a'b'd = \frac{ab}{d}$ с точностью до ассоциативности.

□

11. Билет 11

Далее мы требуем Евклидовости кольца.

Лемма. $\forall a, b, c \in R\colon\ \gcd(a, b) = \gcd(a - bc, b)$.

Доказательство. $\gcd(a, b)R =^{?} \gcd(a - bc, b)R$.

$\gcd(a, b)R = aR + bR$, $\gcd(a - bc, b)R = (a - bc)R + bR$.

"$\supseteq$" $a - bc \in aR + bR, b \in aR + bR$.

"$\subseteq$" $b \in bR \subseteq (a - bc)R + bR$, $a = (a - bc) + bc \in (a - bc)R + bR$. □

Лемма. $\gcd(a, 0) = a$

Замечание. $\gcd(a, b)R = aR + bR = (a,\ b)$, где последнее означает идеал, порождённый a и b.

Поэтому часто наибольший общий делитель обозначают через $(a,\ b)$.

Алгоритм:

$a, b \in R, \nu$ — евклидова норма.

$a = bq_0 + r_0\ b = r_0q_1 + r_1$

...

$r_i = r_{i+1}q_{i+2} + 0$

(Если здесь вам стало плохо, в конспекте лектора есть пояснение в словах. Алгоритм Евклида стр. 36)

Утверждается, что $r_{i+1} = (a, b)$.

$r_0 = 0 \vee \nu(r_0) < \nu(b)$, $(a, b) = (a - bq_0,\ b) = (r_0,\ b) = (b,\ r_0)$

$r_1 = 0 \vee \nu(r_1) < \nu(r_0)$, $(b,\ r_0) = (r_0,\ r_1)$

Также полезен факт, что мы движемся строго по убыванию евклидовой нормы, откуда понятно, что процесс конечен .