МГУ. 1981-1982 уч.г.

ПРОГРАММА

курса общей алгебры, читанной в I семестре

1. Группа. Аксиомы группы. Простейшие свойства. Примеры групп.

2. Подгруппа, порядок группы и элемента, циклические подгруппы. Циклические группы и их описание.

3. Гомоморфизм групп, ядро, образ, простейшие свойства, изоморфизм. Действие группы на множестве. Теорема Кейли.

4. Классификация действий групп на множествах. Транзитивное действие. Теорема Лагранжа.

5. Нормальная подгруппа, фактор-группа, канонический изоморфизм. Классификация гомоморфизмов.

6*. Группа подстановок, транспозиции, циклическая запись, порядки элементов, минимальная система образующих, соотношения, знакопеременная подгруппа A_n. Простота A_n.

7. Малая теорема Ферма.

8. Теорема о числе подгрупп, сопряженных с данной. Центр группы.

9. Две теоремы об изоморфизме.

10. Кольца, поля. Простейшие свойства.

11. Делители нуля. Конечные коммутативные кольца без делителей нуля. Кольца вычетов, случай простого модуля.

12. Морфизмы колец и полей. Идеал, фактор-кольцо, классификация морфизмов колец и полей.

13. Подкольца и подполя, простейшие свойства. Вложимость кольца в кольцо эндоморфизмов абелевой группы.

14. Существование максимального идеала, свойства.

15. Целостные кольца, вложение целостного кольца в поле.

16. Евклидовы и факториальные кольца, кольца главных идеалов. Простейшие свойства и примеры.

17. Теория делимости в целостных кольцах. Теоремы о включениях.

18. Поле рациональных дробей над произвольным полем. Разложение правильной рациональной дроби в сумму простейших. Применение к случаю $P = \mathbb{C}$.

19. Теорема о существовании расширения поля, содержащего корень неприводимого многочлена. Поле разложения для производного многочлена.

20. Поле C.

21. Алгебраические расширения. Простейшие свойства.

22. Существование алгебраически замкнутого расширения. Алгебраическое замыкание. Существование трансцендентных числе.

23. Конечные поля.

24*. Конечно-порожденные абелевы группы.

Обязательно уметь решать задачи из соответствующих разделов Кострикина.

Примечание. Вопросы, помеченные звездочкой, задаются в случае желания экзаменующегося получить хорошую отметку.

Администрация желает студентам хорошо сдать экзамен по общей алгебре.

А Л Г Е Б Р А

Глава 0.

§ I.

I. Считаются известными понятия: множество M, подмножество N, включение $N \subset M$ понимается в не исключающем равенство смысле; $M \cup M_1$, $M_1 \cap M$, дополнение $\overline{N}$ во мн-ве M, $M \setminus N$; операция симметрической разности (Δ): $A \Delta B = (A \setminus B) \cup (B \setminus A)$; свойства операций, например, $A \cap (B \cap C) = (A \cap B) \cap (A \cap C)$ и т.п.

Задача 0. Упростить $((A \cup B) \cap ((A \setminus B) \cap C)) \cup (A \cup (B \setminus C))$.

2. Логические символы $\exists$, $\forall$, $:$, $\Leftrightarrow$, $\Rightarrow$ также считаются известными.

3. Декартовым или прямым произведением мн-в A и B наз. $A \times B = \{(a,b) \mid a \in A, b \in B\}$.

4. Считаются известными понятия отображения $f: S \to T$; $f: s \mapsto t$, $t = f(s)$, $S \xrightarrow{f} T$, другие обозначения этого типа, а также композиция отображ. $g \circ f$, где $f: S \to T$, $g: T \to U$

5. $f: S \to T$ наз. инъективным (мономорфным), если из $x \neq y \Rightarrow f(x) \neq f(y)$.

$f: S \to T$ наз. сюръективным, если $\forall\, y \in T\ \exists\, x: f(x) = y$ (синонимы: эпиморфизм, отображение "на").

$f: S \to T$ наз. биективным или взаимно однозначным (реже изоморфизмом множеств), если f одновременно моно и эпи.

6. Пусть $f: S \to T$; $S_1 \subset S$ образом $f(S_1)$ является $\{y \in T \mid \exists\, x \in S_1,\ f(x) = y\}$

Если $T_I \subset T$. Полный прообраз $f^{-I}(T_I) = \{x \in S \mid f(x) \in T_I\}$.

7. Если f – биекция $S \to T$, то $\exists$ обратное отображение $g \overset{def}{=} f^{-I}: T \to S$; такое, что $f \circ f^{-I} = id_T$, $f^{-I} \circ f = id_S$, где $id_M: M \to M$ – тождественное отображение мн-ва M, т.е. $id_M: x \mapsto x\ \forall x \in M$.

8. Говорят, что элементы мн-ва M занумерованы множеством индексов I, если существует отображение $i: I \to M$.

§ 2. Отношения

Определение Отношением на множестве M наз. любое подмножество $R \subset M \times M$. Обычно, если $(a,b) \in R$ пишут aRb и говорят, что a и b находятся в отношении R.

Замечание. Т.к. отношение R является множеством, то можно говорить о включении отношений R_I R, объединении отношений R_I R, пересечении отношений $R \cap R_I$, дополнении $\overline{R} = (M \times M) \setminus R$.

Примеры. I. Отношение порядка на $\mathbb{N}$, или $\mathbb{Z}$, или $\mathbb{Q}$, или $\mathbb{R}$ $x \leq y$. Св-ва:

I^0 $x \leq x$

2^0 $x \leq y$ и $y \leq z \Rightarrow x \leq z$

Определение. Отношение R на мн-ве M наз. отношением эквивалентности ($aRb \Leftrightarrow a \underset{R}{\sim} b$), если выполнены 3 свойства:

I^0 $a \sim a$ рефлексивность;

2^0 $a \sim b$ и $b \sim c \Rightarrow a \sim c$ транзитивность;

3^0 $b \sim a \Rightarrow a \sim b$ симметричность.

Пример 2. (основной пример отношения эквивалентности). Пусть M разбито в дизъюнктное (не пересекающееся) объединение семейства подмн-в M, т.е. $M = \bigcup_{k \in I} M_k$, $M_k \cap M_i = \emptyset$.

Введем отношение $aRb \overset{def}{\Leftrightarrow} a, b \in M_k$. Проверим свойства:

I^0 $aRa \Leftrightarrow a \in M_k$ и $a \in M_k$.

2^0 $a\,R\,b$ и $bRc \Leftrightarrow a,b \in M_к$; $b,c \in M_к \Rightarrow a,c \in M_к \Leftrightarrow aRc$.

3^0 $aRb \Leftrightarrow a,b \in M_к \Leftrightarrow b,a \in M_к \Leftrightarrow bRa$. Следовательно, R – отношение эквивалентности.

Утверждение. Всякое отношение эквивалентности является отношением типа примера 2, т.е. разбивает мн-во M на непересекающиеся подмн-ва.

Д-во. Определим мн-во $\bar{a} = \{x \in M \mid x \underset{R}{\sim} a\}$

I. $a \underset{R}{\sim} a \Leftrightarrow a \in \bar{a}$. 2. Два мн-ва $\bar{a}$ и $\bar{b}$ либо не пересекаются либо совпадают. $\overline{c \wedge \bar{a} \cap \bar{b} \neq \emptyset} \wedge c \in \bar{a} \cap \bar{b} \Rightarrow$ а) $a \underset{R}{\sim} c$, $b \underset{R}{\sim} c \Rightarrow a \underset{R}{\sim} b$; в) $e \in \bar{a} \Leftrightarrow e \underset{R}{\sim} a$, но $a \underset{R}{\sim} b \Rightarrow e \underset{R}{\sim} b \Rightarrow e \in \bar{b}$ и наоборот $\Rightarrow \bar{a} = \bar{b}$.

Замечание I. Про мн-во $\bar{a}$ говорят "класс эквивалентности элемента a".

2. Рассмотрим мн-во классов эквивалентности $M/R \overset{def}{=} \{M_к \subset M \mid M_к$ – чей-то класс эквивалентности, и всякий класс входит только один раз$\}$. M/R наз. мн-вом классов эквивалентности.

Пример 3. Построение $\mathbb{Z}$. Рассмотрим $\mathbb{N}$ и введем на мн-ве $\mathbb{N} \times \mathbb{N}$ отношение эквивалентности: $(a_I,b_I) \underset{\mathbb{Z}}{\sim} (a_2,b_2) \Leftrightarrow a_I+b_2 = a_2+b_I$. $\mathbb{N}\times\mathbb{N}/\underset{\mathbb{Z}}{\sim}$ наз. $\mathbb{Z}$

Введем операции:

1. $(\overline{a_I,b_I})+(\overline{a_2,b_2}) = (\overline{a_I + a_2,\ b_I + b_2})$.
2. $(\overline{a_I,b_I})\cdot(\overline{a_2,b_2}) = (\overline{a_Ia_2 + b_Ib_2,\ a_Ib_2 + b_Ia_2})$.

Необходимо проверить корректность операций (т.е. класс эквивалентности, полученный в результате операции, будет одним и тем же для всякого представителя исходных классов эквивалентности):

I. $(c_I,\ e_I) \underset{\mathbb{Z}}{\sim} (a_I,b_I) \Leftrightarrow c_I+b_I = e_I+a_I$.
$(c_2,\ e_2) \underset{\mathbb{Z}}{\sim} (a_2,b_2) \Leftrightarrow c_2+b_2 = e_2+a_2$.

$(\overline{a_I,b_I}) + (\overline{a_2,b_2}) = (\overline{a_I+a_2, b_I+b_2})$; $(\overline{c_I,e_I}) + (\overline{c_2,e_2}) = (\overline{c_I+c_2, e_I+e_2})$.

$a_I+a_2+e_I+e_2 = c_I+c_2+b_I+b_2 \Leftrightarrow (a_I+a_2, b_I+b_2) \underset{\mathbb{Z}}{\sim} (c_I+c_2,\ e_I+e_2)$.

Так же проверяется и 2.

Задача 2. а) Дистрибутивны ли введенные операции ?
, Проверить остальные свойства .

Замечание. $(\overline{a,b})$ есть на самом деле a–b, например, класс (a,a) соответствует нулю (является нулем).

Пример 4. Построение $\mathbb{Q}$. Рассмотрим $\mathbb{Z}$ и на мн-ве $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ введем отношение эквивалентности $(a_I,b_I) \underset{\mathbb{Q}}{\sim} (a_2,b_2) \Leftrightarrow a_Ib_2 = a_2b_I$. $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})/\underset{\mathbb{Q}}{\sim}$ наз. $\mathbb{Q}$.

Задача 2 б) Ввести в $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})/\underset{\mathbb{Q}}{\sim}$ операции и проверить все свойства $\mathbb{Q}$.

Таким образом, считаются известными множества $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ и их основные свойства.

Глава I

§ I. Операции на множествах. Группа. Примеры, простейшие свойства и конструкции.

Алгебра изучает мн-во с заданными на нем одной или несколькими операциями.

Определение n-арной операцией на мн-ве M наз. $f: \underbrace{M\times M\times\ldots\times M}_{n \text{ раз}} \to M$.

При n= I говорят об унарной операции, n=2 – бинарной и т.д.

Пример. I) M – числовая система ($\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$). $x \mapsto x^n$, где n – фиксировано.
2) M – то же. $x \mapsto -x$,
3) $A \in Mat_n(\mathbb{R})$, и $A \xrightarrow{f} A^T$
4) $M = \{\mathbb{Q}\setminus\{0\},\ \mathbb{R}\setminus\{0\},\ \mathbb{C}\setminus\{0\}\}$, $x \mapsto x^{-I} = I/x$.

Унарные операции примеров 2÷ 4 обладают тем свойством, что $f^2 = f \circ f = id_M$
Отображения(или операции), обладающие этим св-вом наз.инволюцией.

Определение Группой G наз. мн-во с заданной на нем бинарной операцией, т.е. отображением $f: M \times M \to M$ $(a,b) \mapsto c$ (обычно используется обозначение $ab=c$ или, если хотят подчеркнуть особенность операции, $a \circ b = c$, $a \otimes b = c$), удовлетворяющей 3-м свойствам (аксиомам группы):

1^0 $(a \circ b) \circ c = a \circ (b \circ c)$ /ассоциативность операции/;!

2^0 $\exists e \in G: \forall a \in G$ $ae = ea = a$ /существование единицы, нейтрального элемента/;

3^0 $\forall a \in G$ $\exists a^{-1} \in G: aa^{-1} = a^{-1}a = e$ /существование обратного эл-та/

Замечание. Если в группе G операция, кроме указанных, удовлетворяет дополнительному свойству: 4^0 $ab = ba$, то такая группа наз. абелевой или коммутативной. Часто для коммутативных групп употребляется аддитивная запись: операция обозначается "+" ($a + b = c$); единичный элемент называется нулем 0, и свойство 2^0 записывается так: $a + 0 = a$; обратный элемент наз. противоположным; св-во 3^0 записывается: $a + (-a) = 0$.

Простейшие св-ва группы:

1. Единица в группе единственна. Действительно, если e_1 и e_2 - две единицы группы, то $e_1 = e_1 e_2 = e_2 = e$.

2. Любая односторонняя единица совпадает с единицей. Если $e_1 a = a$, то $e_1 = e_1 e = e$.

3. Обратный элемент единственен. Действительно, если $b_1 a = e$ и $ab_2 = e$, то $b_1 = b_1 a b_2 = b_2 = a^{-1}$.

4. Односторонний обратный совпадает с обратным. Док-во аналогично.

5. Уравнения $ax=b$ и $ya=b$ имеют единств. решение. $ax=b$ умножим на a^{-1} слева. Тогда $x = a^{-1}b$ и т.п.

Задача 3. Определение группы 2. Группой G наз. мн-во с бинарной операцией, обладающей след.свойствами:

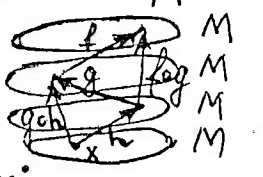
1. ассоциативность операции.
2. всякое уравнение $ax=b$ или $ya=b$ имеет единственное решение.

Определение группы 3. Группой G наз. мн-во с бинарной операцией, обладающей след.св-вами:

1. Операция ассоциативна.
2. Существует правая единица: $ae=a$ $\forall a \in G$
3. Существует правый обратный: $\forall a \in G \exists a^{-1}$, что $aa^{-1} = e$.

Доказать, что все три определения эквивалентны.

Примеры: I. $Bi(M) = \{f: M \to M \mid f$ - биекция$\}$ - группа относительно операции композиции. 1^0



$f \circ (g \circ h) = (f \circ g) \circ h$
$\forall x \in M$

2^0 $e = id_M$;
3^0 $\forall f \in Bi(M)$ $\exists f^{-1}: f \circ f^{-1} = f^{-1} \circ f = id_M$

Как станет ясно потом, этот пример в некотром смысле"главный".

2. M - метрическое пространство; $f: M \to M$, так, что $\rho(x,y) = \rho(f(x), f(y))$ наз. изометрией. Пусть $Iso(M) = \{f$ - изометрия и биекция$\}$. Ясно, что $Iso(M) \subset Bi(M)$, $Iso(M)$ - группа относительно операции композиции отображений.

3. Замечания о структурах

Если множество M обладает какой-то"структурой", то все биекции M, сохраняющие эту"структуру", образуют группу по композиции. Например, топология и гомеоморфизмы, дифференцируемые многообразия и диффеоморфизмы, метрические пространства и изометрии и т.д.

4. M– правильный n-угольник, $Д_n$ – группа движений правильного n-угольника. Группа эта состоит из элементов двух сортов: поворотов и отражений. Эта Группа наз. группой диэдра.

5. M – правильный многогранник (тетраэдр, куб, октаэдр, икосаэдр, додекаэдр. Можно изучать группы движений прав.многогранников. Эта также не сложно.

6. Пусть M – конечное мн-во. Занумеруем его элементы $1,2,\dots,n$. Тогда $B\,i(M) = S_n$ наз. симметрической группой из n элементов. Эл-ты $\sigma \in S_n$ наз. подстановками. Всякая подстановка $\sigma \in S_n$ указывает, куда переходит эл-т K, именно $\sigma : k \to \sigma(k)$. Это можно записать в две строчки: $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$.

Произведение подстановок определяется как композиция:например, для S_3

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$. Обратный элемент действует как обратное отображение. Эта группа не коммутативна. (Проверьте!)

Примеры другого характера.

7. $(\mathbb{Z}, +)$; $(\mathbb{Q}, +)$; $(\mathbb{R}, +)$.

8. $(\mathbb{R}\setminus\{0\}, \cdot)$; $(\mathbb{R}\setminus\{0\}, \cdot)$; $(\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}, \cdot)$.

9. $(\{1, -1\}, \cdot)$.

10. Рассмотрим $\mathbb{Z}$ и введем на нем отношение эквивалентности $\underset{2}{\sim}$: $a \underset{2}{\sim} b \iff a - b \vdots 2$ (или $2 \mid (a - b)$). $\mathbb{Z}/\underset{2}{\sim}$ состоит из 2-х классов. В одном есть 0, класс $\bar{0}$, во втором – 1, класс $\bar{1}$. Операция: $\bar{a} + \bar{b} = \overline{(a+b)}$.

Проверим корректность определения: $a \underset{2}{\sim} a_1 \iff a - a_1 = 2k$

$$b \underset{2}{\sim} b_1 \iff b - b_1 = 2m. \Rightarrow$$

$a + b - (a_1 + b_1) = 2(k + m) \Rightarrow a + b \underset{2}{\sim} a_1 + b_1$.

Теперь проверим групповые свойства:

1^0 ассоциативность вытекает из свойств $\mathbb{Z}$.

2^0 $e = \bar{0}$.

3^0 $(\bar{1})^{-1} = (\bar{1})$.

И вообще, все это видно из такой таблицы (таблицы Кели):

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

Замечание: По такой таблице хорошо видно существование e, a^{-1}, коммутативность. Но плохо проверять ассоциативность.

11. $Ц_n$ – циклическая группа порядка n. а) $Ц_n = \{e, a, a^2, \dots, a^{n-1} \mid a^k a^m = a^{k+m},\ na^n = e\}$

б)

·	e	a	a^2	a^3	…	a^{n-1}
e	e	a	a^2	a^3	…	a^{n-1}
a	a	a^2	a^3	a^4		e
a^2	a^2	a^3	a^4	a^5		a
a^3	a^3	a^4	a^5	a^6		a^2
⋮	⋮	⋮	⋮	⋮		⋮
a^{n-1}	a^{n-1}	e	a	a^2		a^{n-2}

I2. V_4 - vierer gruppe Klein

	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	1	e_3	e_2
e_2	e_2	e_3	1	e_1
e_3	e_3	e_2	e_1	1

I3. Движения плоскости: повороты и параллельные переносы (сдвиги).

I4. Векторы.

I5. $\mathbb{R}$ и $\mathbb{R}\times\mathbb{R} = \{(a,b) \mid a,b\in\mathbb{R}\}$. Введем операцию: $(a_I,b_I)+(a_2,b_2) = (a_I+a_2, b_I+b_2)$. Говорят, что таким образом введенная операция (в данном случае сложение) вводится покоординатно. Проверка свойств осуществляется непосредственно.

Задача 4. Дано мн-во, M на котором введены операции: объединение, пересечение и симметрическая разность его подмножеств. Какие из них определяют группу ?

Конструкция

Определение Пусть $(G,*)$ и $(H,\circ)$ - две группы. Прямым произведением $G\times H$ наз. группа, элементы которой - элементы прямого произведения множеств $G\times H = \{(g,h) \mid g\in G,\ h\in H\}$, а операция вводится покоординатно: $(g_1,h_1)\cdot(g_2,h_2) = (g_1*g_2, h_1\circ h_2)$; $e = (e_I,e_2)$, где e_I - единица G, e_2 - единица H, обратный элемент $(g,h)^{-I} = (g^{-1}, h^{-1})$. Свойства проверяются легко.

Вообще, если $G_к$, $к\in I$ - конечное семейство групп, то $G_I\times G_2\times\ldots\times G_п = \prod_{к\in I} G_к$ с покоординатным умножением наз. прямым произведением групп $G_к$, $к\in I$.

Эта конструкция позволяет строить новые группы по уже имеющимся; пример I5 $\mathbb{R}\times\mathbb{R}$ является прямым произведением групп $\mathbb{R}$ и $\mathbb{R}$.

Замечание: Рассмотрим подмножества $Iso(M)\subset Bi(M)$; $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}$; $\mathbb{Q}\setminus\{0\}\subset\mathbb{R}\setminus\{0\}$. Видно, что операция не выводит за пределы рассматриваемого подмножества. Т.е. здесь меньшее множество само является группой относительно той же операции.

Определение: $(G,*)$ группа. Помн-во $H\subset G$ наз. подгруппой, если:

1) $\forall a,b\in H \Rightarrow a*b\in H$.
2) $e\in H$.
3) $\forall a\in H \Rightarrow a^{-I}\in H$. (т.е. подмн-во - само группа)

Замечание $(\mathbb{R},+)$, $(\mathbb{Q}\setminus\{0\},\cdot)$ не являются подгруппами.

Задача 5. Доказать, что подмн-во $H\subset G$ является подгруппой $\Leftrightarrow$ $a,b\in H \Rightarrow ab^{-I}\in H$.

Задача 6. H_I, H_2 - подгруппы G. Доказать, что $H_I\cap H_2$ - подгруппа в G. Будет ли объединение двух подгрупп снова подгруппой ? Если нет, привести пример.

Задача 7. Док-ть, что порядок $|S_п| = п!$

Пример I. S_3 состоит из 6 элементов.

Цикловая запись подстановки: $\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n)\end{pmatrix} \leftrightarrow (1\ \sigma(1)\ \sigma(\sigma(1))\ldots)(\ldots)$,

например, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3\end{pmatrix} \leftrightarrow (14)(2)(35) = (14)(35)$

Запись вида: $(1\ \sigma(1)\ \sigma(\sigma(1))\ldots\ )$ - наз. циклом .

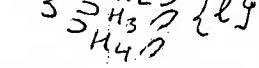
Определение. Порядком элемента $g\in G$ наз. наименьшее число п, такое что $g^{п} = e$. Если такового не существует, то говорят, что эл-т g бесконечного порядка.

Задача 8. Чему равен порядок цикла ? В терминах циклов сформулировать, "чему равен порядок подстановки ?"

(I4) (35) = (I4)o(35) можно рассматривать как произведение двух циклов.

Задача 9. Как в терминах циклов двух подстановок σ_1 и σ_2 сформулировать их перестановочность, т.е. что $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

Итак: $S_3 = \{e, (12), (13), (23), (123), (132)\}$. При этом (12), (13) и (21) – элементы 2-го порядка, а (123) и (132) – третьего порядка.

Подгруппы S_3: $\{e\}$; $\{e,(12)\} = H_1$, $|H_1| = 2$; ...; $\{e,(123),(132)\} = A_3$, $|A_3| = 3$. Структура подгрупп $\longrightarrow$ 

Задача 10. Описать все подгруппы S_4.

Пример 2. X мн-во $\supset$ Y. G – подгруппа $Bi(X)$. Нормализатором Y в G наз. $N_G(Y) = \{g \in G \mid gY \subset Y\}$. Если Y = a, то $N_G(a) = Stab_G(a) = G_a$ наз. стабилизатором a или стационарной подгруппой точки a.

Пример. X – плоскость, G – группа всех собств. движений плоскости (т.е. повороты и параллельные переносы). Тогда $N_G(a) = \{$повороты вокруг точки a$\}$. Этот пример является в некотором смысле основным.

Задача 11. $Z_G(Y) = \{g \in G \mid \forall y \in Y \quad g(y) = y\}$ наз. централизатором Y в G. Доказать, что $Z_G(Y) = \bigcap_{y \in Y} N_G(y)$

Взглянув на все примеры, можно заметить, что многие группы "очень похожи". Например, $(\{1,-1\},\cdot)$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}_2$. (Вспомните таблицы Кели для этих групп.)

В алгебре мы не интересуемся природой элементов и операций. Нас интересуют основные свойства операции.

Определение. Биекция $\varphi : (G, \circ) \to (H, *)$ наз. изоморфизмом, если

$$\forall g_1, g_2 \in G \quad \varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2).$$

Группы G и H наз. изоморфными, если $\exists$ хотя бы один изоморфизм $\varphi : G \to H$.

Задача 12. Если $\varphi : G \to H$ изоморфизм, то $\varphi^{-1} : H \to G$ тоже изоморфизм.

Изоморфизм $\varphi : G \to G$ наз. автоморфизмом.

Общее замечание об автоморфизмах.

$Aut\ G = \{\varphi$: автоморфизм $\varphi : G \to G\}$-группа.

Пример. 1. $G = (\mathbb{R}, +)$; $H = (\mathbb{R} \setminus \{0\}, \cdot)$. $\varphi : G \to H$ определяется так: $\varphi(a) = e^a$. Свойства $\varphi(a + b) = e^{(a+b)} = e^a \cdot e^b = \varphi(a) \cdot \varphi(b)$ – отчасти выполняются, но φ не является сюръекцией ($\varphi(G) = \mathbb{R}_+$), т.е. не является и биекцией.

Пример 2. $\varphi : \mathbb{Z} \to \mathbb{Z}/2$, $\varphi : a \mapsto \bar{a}$. Св-во $\varphi(a + b) = \varphi(a) + \varphi(b)$ выполняется, и φ – сюръективно, но не инъективно.

Определение. $\varphi : (G, \circ) \to (H, *)$ наз. гомоморфизмом группы G в H, если

$$\forall g_1, g_2 \in G \quad \varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2).$$

Мономорфизм – это гомоморфизм, осуществляющий взаимно-однозначное отображение; эпиморфизм – это гомоморфизм "на".

Простейшие свойства.

1. $\varphi(e_G) = e_H$; 2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$; 3. Образ φ является подгруппой в H.

Пример 3. (основной) Определение. G – группа и M – множество. Действием группы на множестве M наз. гомоморфизм $\varphi : G \to Bi(M)$.

Другое определение. Действием (левым) группы G на M наз. $\mathcal{F} : G \times M \to M$, точнее, $\mathcal{F}(g, m) \underset{\text{обозн}}{\overset{def}{=}} gm$ со свойствами: $g_1(g_2 m) = (g_1 g_2)m$, $em = m$ $\forall m \in M$.

$g: M \to M$ и $\sigma_g: m \mapsto gm$. σ_g определено, $(\sigma_g)^{-1} = \sigma_{g^{-1}} \Rightarrow \sigma_g$ – биекция.
$\sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2} \Rightarrow \varphi: g \longmapsto \sigma_g$ – гомоморфизм.

Пример 4. Группа G действует на себе левыми сдвигами: $\forall g_1 \in G \quad L_{g_1}: G \to G \Leftrightarrow$
$\Leftrightarrow L_{g_1}(g) = g_1 g$ Проверим, что это действие G на G.

1. $L_e(g) = eg = g \ \forall g \Rightarrow L_e = id_G$
2. $L_{g_1 g_2}(g) = (g_1 g_2)g = g_1(g_2 g) = L_{g_1}(g_2 g) = L_{g_1}(L_{g_2}(g)) = L_{g_1} \cdot L_{g_2}(g)$

Можно аналогично определить правый сдвиг: $\forall g_1 \in G \quad R_g: G \to G \Leftrightarrow R_{g_1}(g) = gg_1^{-1}$
При этом $g \mapsto R_g$ – гомоморфизм. Если определить $\overline{R}_{g_1}: G \to G \quad \overline{R}_{g_1}(g) = gg_1$, то это не будет действием в нашем определении. Говорят о "правом действии".

Следствие. Теорема Кэли (Cayley)(Кейли). Всякая группа G изоморфна подгруппе $Bi(G)$. Док-во. Надо д-ть, что $\varphi: g \mapsto L_g$ – моно(взаимно однозначно). Действительно, $L_{g_1} = L_{g_2} \Leftrightarrow \forall g \ L_{g_1}(g) = L_{g_2}(g) \Leftrightarrow g_1 g = g_2 g \Rightarrow g_1 = g_2$

Следствие. $|G| = n$, то $G \hookrightarrow S_n$.

Задача 15. $G = V_4$. Описать $\varphi: G \hookrightarrow S_4$.

Задача 16. В какие S_n вкладываются группы движений правильных многогранников?

Мы находимся в ситуации, когда G действует на M. Введем отношение эквивалентности $m_1 \sim m_2 \Leftrightarrow \exists g \in G \ gm_1 = m_2$ (проверьте, что это отношение экв.). Класс эквивалентности называется орбитой элемента g.

Лекция 3. § 5. Классификация действий групп на множествах

Постараемся изучить более подробно действие G на M.

Пример 1. G – группа поворотов плоскости вокруг точки $\{0\}$. Любую ли точку $x \in M$ можно перевести в другую? Ясно, что нет. Пусть $x=(x_1, x_2)$ – координаты точки x, $|x|^2 = x_1^2 + x_2^2$, тогда $|x| = |gx|$ для $\forall g \in G$. Каждая точка скользит по своей окружности.

Определение 1. G действует на M. Введем на M отношение эквивалентности: $x \sim y \Leftrightarrow \exists g \in G$ такое, что $gx = y$ (проверьте, что это – отношение эквивалентности). Класс эквивалентности элемента x наз. орбитой элемента x и обозначается o_x. В соответствии со свойствами отношения эквивалентности все множество M разбивается в объединение непересекающихся орбит. В примере 1 орбитами являются окружности с центрами в 0 и точка 0. Видно, что орбиты могут быть топологически "очень непохожими".

Определение 2. Говорят, что G действует на M транзитивно, или, что M является однородным G – пространством, если для любых двух $x, y \in M \ \exists g \in G$ такое, что $gx = y$.

Ясно, что G действует на o_x транзитивно.

Пример 2. S_3 действует на множестве $M = \{1,2,3\}$ транзитивно. Разберем этот пример подробнее: а) фиксируем элемент $x_0 = \{2\} \in M$. Вся группа S_3 разбивается на 3 множества M_1, M_2, M_3 по тому, куда переводится элемент x_0.

$M_1 = \{(12), (132)\}$; $M_2 = \{e, (1,3)\}$; $M_3 = \{(23), (123)\}$.

Из этих подмножеств только $M_2 = N_G(2) = G_2$ – является подгруппой (стационарной подгруппой (стационарная подгруппа элемента x_0).

Множества M_1 и M_3 получаются так: в каждом из этих множеств можно выбрать по элементу (любому) $g_1 \in M_1$ и $g_3 \in M_3$ и $M_1 = L_{g_1}(M_2)$, $M_3 = L_{g_3}(M_2)$ /Проверьте!/. Рассмотрим другой элемент $x_1 = 3 \in M$. Чтобы получить разбиение, соответствующее этому элементу, нужно провести "перенумерацию" $f: M \to M$ такая, что $f(1)=1$; $f(2)=3$; $f(3)=2$. $N_1 = \{(3)(1\ 2)\}$, $N_2 = \{(3\ 2) = (2\ 3)(1\ 3\ 2)\}$, $N_3 = \{e\ (1\ 2)\}$.

$N_3 = N_G(3) = G_3$ – стационарная подгруппа элемента x_1. Как можно получить G_3 из G_2? Возьмем произвольный $g \in S_3$ такой, что $g(3)=2$. Тогда $G_3 = g^{-1} G_2 g$ /Проверьте это.) Этот пример подсказывает следующие определения и утверждения.

Определение 3. Пусть G действует на X и Y. Действия G называются изоморфными (эквивалентными), если $\exists$ биекция $\varphi: X \to Y$ такая, что для всех $g \in G$ и $x \in X$ $\varphi(gx) = g\varphi(x)$.

Как это определение соотносится с определением действия, как гомоморфизма $\varphi: G \to Bi(X)$?

Определение 4. $f: X \to Y$ – биекция, тогда f индуцирует гомоморфизм f_*: $i(X) \to Bi(Y)$. Таким образом, $S \in Bi(X)$ $f_*(S) = f \circ S \circ f^{-1}$, или $f_*(S) \in Bi(Y)$ так что $\forall S$ диаграмма $\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow S & & \downarrow f_*(S) \\ X & \xrightarrow{f} & Y \end{array}$ коммутативна (проверьте, что f_* – гомоморфизм).

/Примечание: диаграмма коммутативна, если результат операций не зависит от пути. Например, в условиях нашей диаграммы это означает, что $f \circ S = f_*(S) \circ f$ /.

Определение 5. Пусть $\varphi: G \to Bi(X)$; $\Psi: G \to Bi(Y)$ – действия G в X и, соответственно, в Y. Говорят, что они изоморфны (эквивалентны), если $\exists f: X \to Y$ биекция, такая, что диаграмма $\begin{array}{ccc} & & Bi\,X \\ & \varphi \nearrow & \downarrow f_* \\ G & & \\ & \Psi \searrow & Bi\,Y \end{array}$ коммутативна.

Лемма 1. Определения 3 и 5 эквивалентны.

Доказательство леммы состоит из аккуратного выписывания определений.

Определение 6. G – группа, H – ее подгруппа. Введем в G отношение эквивалентности $a \sim b \Leftrightarrow a^{-1} b \in H$. Класс эквивалентности по этому отношению назовем левым смежным классом по подгруппе H. Множество левых смежных классов обозначается G/H.

G действует на мн-ве G/H транзитивно левыми сдвигами: $L_g(g_1 H) = g g_1 H$. Проверим корректность этой конструкции. Пусть $a \sim b \Leftrightarrow a^{-1} b \in H$. Докажем, что $ga \sim gb$. Действительно, $(ga)^{-1}(gb) = a^{-1} g^{-1} g b = a^{-1} b \in H \Leftrightarrow ga \sim gb$. (Проверьте транзитивность сами.)

Утверждение $\forall$ два смежных класса равномощны. Д-во: $g_1 H = (g_1 g_2^{-1}) g_2 H$.

Следствие 1. Теорема Лагранжа. G – конечная группа, H – ее подгруппа. Тогда $|H| \mid |G|$ (порядок группы делится на порядок подгруппы). Число классов G/H $(G:H) = [G:H]$ и называется индексом H в G.

Следствие 2. G – конечная группа. Тогда для любого $g \in G$ порядок g делит порядок группы G (обозначение: $\operatorname{ord} g$. Точнее формулировка: $\operatorname{ord} g \mid |G|$).

Это непосредственное следствие теоремы Лагранжа.

Замечание: обращение теоремы Лагранжа неверно. (Вспомните задачу о подгруппах группы S_4)

Задача 18. Введем в G другое отношение эквивалентности: $a \sim b = ab^{-1} \in H$. Классы эквивалентности по этому отношению называются правыми смежными классами. Класс обозначается Hg, множество классов $H \backslash G$. Доказать, что $|H \backslash G| = [G:H]$ (индекс правый = индексу левому).

Указание: в любой группе есть биекция $f: G \to G$ $f: x \to x^{-1}$. f не является автоморфизмом ! Как f действует на левых смежных классах по H ?

Следствие 3. G – конечная группа такая, что $|G| = p$ – простое число. Тогда G изоморфна $\mathbb{Z}_p$ (с точностью до изоморфизма существует только одна конечная группа простого порядка – циклическая). Док-во. Пусть $g \in G$ и $g \neq e$. Тогда G совпадает с циклической подгруппой, порожденной элементом g. Все.

Задача 19. Найти все конечные группы (с точностью до изоморфизма) такие, что $|G| < 6$. Докажите, что они все абелевы.

Теорема 1. Любое транзитивное действие G на X эквивалентно действию G на G/H. (для некоторой H).

Док-во. Фиксируем $x_0 \in X$. Пусть $H = N_G(x_0) = G_{x_0}$ – стационарная подгруппа. $Y = G/H$. Определим отображение $f: X \to Y$ таким образом: $\forall\, x_1 \in X\ \exists g: x_0 \mapsto x_1$ (транзитивность действия) положим $f(x_1) = \{gH\} \in Y$.

а) проверим корректность: пусть g_1 – другой элемент группы такой, что $g_1 : x_0 \mapsto x_1$, тогда $g_1^{-1} g : x_0 \xrightarrow{g} x_1 \xrightarrow{g_1^{-1}} x_0 \Rightarrow g_1 \sim g$. Следовательно, образ $f(x_1)$ не зависит от выбора g. Кроме того, мы получили, что любой левый смежный класс $gH = \{g_1 \in G \mid g_1 x_0 = x_1\}$.

Докажем теперь изоморфизм (эквивалентность) действий G на X и на Y. Нам надо доказать, что $\forall\, g_1 \in G$ и $x_1 \in X$ $f(g_1 x_1) = g_1 f(x_1)$. (Напоминаем, что по прежнему фиксирована точка x_0.) Пусть $g: x_0 \mapsto x_1$, $g_1: x_1 \mapsto x_2$, тогда $g_1 g : x_0 \mapsto x_1$, По построению f $f(x_1) = gH$ $f(x_2) = f(g_1 x_1) = g_1 gH$, а $g_1 f(x_1) = g_1 gH$, т.е. $f(g_1 x_1) = g_1 f(x_1)$. Вся эта проверка определений хорошо видна из следующей диаграммы:

$$\begin{array}{ccccc} x_0 & \xrightarrow{g} & x_1 & \xrightarrow{g_1} & x_2 \\ \downarrow f & & \downarrow f & & \downarrow f \\ H & \longrightarrow & gH & \xrightarrow{g_1} & g_1 gH \end{array}$$

Лекция 4.

Определение 6. Внутренним автоморфизмом или "сопряжением" называется $A_g: G \to G$: $A_g(x) = g x g^{-1}$. Проверим, что это автоморфизм: $A_g(x_1 x_2) = g x_1 x_2 g^{-1} = g x_1 g^{-1} g x_2 g^{-1} = (g x_1 g^{-1}) \cdot (g x_2 g^{-1}) = A_g(x_1) \cdot A_g(x_2)$. Множество внутренних автоморфизмов обозначается $Int\, G$.

Задача 20. $Int\, G$ подгруппа в $Aut\, G$. В частности, $(A_g)^{-1} = A_{g^{-1}}$

Задача 21. G – абелева $\Leftrightarrow$ $Int\, G = \{e\}$.

Теорема 2. Действие G на G/H_1 и G/H_2 эквивалентны $\Leftrightarrow$ H_1 и H_2 сопряжены в G (т.е. получаются друг из друга некоторым внутренним автоморфизмом).

Док-во: Если H_1 – стабилизатор x_1, H_2 – стабилизатор x_2, причем $g x_1 = x_2$, то $\forall h_1 \in H_1$ $g h_1 g^{-1} x_2 = x_2 \Rightarrow g h_1 g^{-1} \in H_2$

Обратно. Если $H_1 = g H_2 g^{-1}$, то правый сдвиг $R_g : x \mapsto xg$ переводит G/H_1 в G/H_2 и коммутирует с действием (проверьте это).

§ 6. Классификация гомоморфизмов. Нормальные подгруппы.

В предыдущем параграфе мы описали в некотором смысле (в терминах группы) любое действие группы G на множестве X. Постараемся теперь описать гомоморфизмы $\varphi: G_1 \to G_2$.

1. Любой гомоморфизм $\varphi: G_1 \to G_2$ раскладывается как $G_1 \xrightarrow{\hat{\varphi}} \varphi(G_1) \xrightarrow{i} G_2$, где i – вложение $\varphi(G_1)$ подгруппы в G_2, т.е. φ раскладывается в композицию

эпиморфизма $\hat{\varphi}$ и мономорфизма (вложения). Задать мономорфизм $G_1 \hookrightarrow G_2$ все равно, что задать подгруппу G_1 в G_2. Постараемся описать эпиморфизмы.

Пусть $G \xrightarrow{\varphi} X$, φ – эпиморфизм групп. Что такое $\varphi^{-1}(x)$?

Определение. $\mathrm{Ker}\,\varphi = \{g \in G \mid \varphi(g) = e\}$ наз. ядром гомоморфизма φ.

Утверждение. $\varphi : G \to X$ эпиморфизм; если $H = \mathrm{Ker}\,\varphi$, то $\varphi^{-1}(x) = gH$ для некоторого $g \in G$. Доказать это самостоятельно.

Отсюда получается, что прообразы точек – это смежные классы G/H, т.н. X (пока как множество) совпадает с G/H, где $H = \mathrm{Ker}\,\varphi$. Но X – группа, в X есть умножение. Каким должно быть умножение на G/H, чтобы оно совпадало с умножением в X? $\varphi : g_1 H \mapsto \varphi(g_1)$, $\varphi : g_2 H \mapsto \varphi(g_2)$, $\varphi(g_1)\cdot\varphi(g_2) = \varphi(g_1 g_2)$.

Следовательно, $(g_1H)\otimes(g_2H) = g_1g_2H \Longleftrightarrow g_1g_2(g_2^{-1}Hg_2)H = g_1g_2H \Longleftrightarrow g_2^{-1}Hg_2 = H$, т.е. подгруппа H должна быть инвариантной при сопряжениях.

Определение. Подгруппа $H \subset G$ наз. нормальной подгруппой (синонимы: нормальный делитель, инвариантная подгруппа) и обозначается $H \lhd G$, если $\forall\, g \in G$ $gHg^{-1} = H$.

Замечание. Не обязательно каждый элемент h остается на месте. Вся группа как множество должна остаться на месте.

Утверждение. Если $\varphi : G_1 \to G_2$ – гомоморфизм, то $H = \mathrm{Ker}\,\varphi \lhd G_1$.

Упражнение. Если $H \lhd G$, то левые и правые смежные классы по H совпадают.

Задача 22. H – подгруппа в G, такая что $[G:H] = 2$. Тогда $H \lhd G$.

Задача 23. Пусть H – единственная подгруппа в G данного порядка; тогда $H \lhd G$. (Посмотрите S_4.)

Задача 24. $G \supset G_1$, $H \lhd G \Rightarrow H \cap G_1 \lhd G_1$.

Примеры. 1. G – абелева $\Rightarrow$ всякая подгруппа нормальная.

2. G, $Z_G = \{z \in G \mid zg = gz \ \forall g \in G\}$ наз. центром группы. $Z_G \lhd G$. Д-ть.

3. G, $[G,G] = \{g_1g_2g_1^{-1}g_2^{-1}$ и всевозможные произведения таких элементов, при условии, что $g_1, g_2 \in G\}$ наз. коммутатором группы G.

а) $[G,G]$ – подгруппа G. Проверить это.

б) $[G,G]$ – нормальная подгруппа G. Доказательство просто: $g(g_1g_2g_1^{-1}g_2^{-1})g^{-1} = gg_1g^{-1}\,gg_2g^{-1}\,gg_1^{-1}g^{-1}\,gg_2^{-1}g^{-1} = g_3g_4g_3^{-1}g_4^{-1}$.

Утверждение 1. $H \lhd G$. Введем во мн-ве G/H умножение $g_1H \cdot g_2H = g_1g_2H$. Тогда G/H с введенной операцией группа.

Проверка этого не составляет труда. Заметим, что $\bar{e}$ в G/H это сама H, а $(gH)^{-1} = g^{-1}H$.

Замечание. G/H наз. факторгруппой. Рассмотрим отображение $\Psi : G \to G/H$; $\Psi : g \mapsto gH$, которое любой элемент группы переводит в смежный класс, его содержащий. Это отображение называется канонической проекцией.

Утверждение 2. $\Psi : G \to G/H$ – гомоморфизм. (проверьте это сами.)

Итак, доказана теорема (об эпиморфизме) Пусть $\varphi : G_1 \to G_2$ эпиморфизм. Тогда $\exists$ изоморфизм $G_2 \to G_1/\mathrm{Ker}\,\varphi$ такой, что диаграмма $G_1 \xrightarrow{\varphi} G_2$, $G_1 \xrightarrow{\Psi} G_1/\mathrm{Ker}\,\varphi$ коммутативна. Здесь Ψ – каноническая проекция.

Эта теорема завершает наше исследование: любой эпиморфизм это каноническая проекция на факторгруппу. Следовательно, если $\varphi : G_1 \to G_2$ – гомоморфизм, то φ раскладывается в композицию: $G_1 \xrightarrow{\Psi} G/\mathrm{Ker}\,\varphi \xrightarrow{\sim} \mathrm{Im}\,\varphi = \varphi(G_1) \xrightarrow{i} G_2$. (изоморфизм; вложение (моно))

Старая формулировка теоремы: Факторгруппа по ядру гомоморфизма изоморфна гомоморфному образу группы.

Примеры. 1. Теперь можно оправдать обозначение группы из двух элементов $\mathbb{Z}/2\mathbb{Z}$. $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ подгруппа в $\mathbb{Z}$. $\mathbb{Z}$ – абелева $\Rightarrow 2\mathbb{Z} \lhd \mathbb{Z}$ (можно проверить и непосредственно.) $\mathbb{Z}/2\mathbb{Z}$ состоит из 2-х классов. $2\mathbb{Z} = \mathrm{Ker}\,\varphi$, $\varphi : \mathbb{Z} \to \{\pm 1\}$

– каноническая проекция.

2. Рассмотрим S_n. Построим гомоморфизм /эпи/ $sign : S_n \to \mathbb{Z}/2\mathbb{Z}$. Рассмотрим $F(X_1,\dots,X_n) = \prod_{i<j}(X_i - X_j)$ – многочлен от n переменных. Положим для всякого $\sigma \in S_n$ $(\sigma F)(X_1,X_2,\dots,X_n) = F(X_{\sigma(1)},X_{\sigma(2)},\dots,X_{\sigma(n)})$. Например, при $n=3$ $F(X_1,X_2,X_3)=(X_3-X_2)(X_3-X_1)(X_2-X_1)$, $(\sigma F)(X_1,X_2,X_3) = (X_{\sigma(3)}-X_{\sigma(2)})(X_{\sigma(3)}-X_{\sigma(1)})\cdot(X_{\sigma(2)}-X_{\sigma(1)}) = (X_2-X_3)(X_2-X_1)(X_3-X_1)$, если $\sigma \in S_3$ и $\sigma=(23)$

Положим $sign\,\sigma = (\sigma F)/F$. /Здесь $\mathbb{Z}/2\mathbb{Z}$ задана в мультипликативной реализации: $\{1,-1;\cdot\}$/ В условиях примера $sign\,\sigma = \frac{(X_2-X_3)(X_2-X_1)(X_3-X_1)}{(X_3-X_2)(X_3-X_1)(X_2-X_1)} = -1$.

$sign\,\sigma\tau = \frac{(\sigma\tau F)}{F} = \frac{\sigma\tau F}{\tau F}\cdot\frac{\tau F}{F} = \frac{\sigma F}{F}\cdot\frac{\tau F}{F} = sign\,\sigma \cdot sign\,\tau$.

Если $sign\,\sigma = 1$, то подстановка σ наз. четной, в противном случае – нечетной. $Ker\,sing = A_n$ и называется знакопеременной группой. A_n состоит из всех четных подстановок.

Упражнение. Найти и изучить еще 5 нетривиальных примеров ситуации группа и нормальная подгруппа.

Лекция 5. § 7. Применения.

1. Рассмотрим группу $\mathbb{Z}/m\mathbb{Z}$. В этой группе есть не только операция сложения, но и операция умножения. Действительно, $(a+km)(b+cm) = ab + (kb+ac+kcm)\cdot m$. Какие же элементы в $\mathbb{Z}/m\mathbb{Z}$ составляют группу по умножению? Ясно, что $\bar{0}$ к ним не принадлежит, единицей является класс $\bar{1}$. Когда найдется обратный эл-т

Лемма. $\bar{a}$ обратим в $\mathbb{Z}/m\mathbb{Z}$ по умножению $\Leftrightarrow$ НОД $(a,m) = 1$.

1) если $\bar{a}$ обратим, то $\exists\, \bar{x}$: $\bar{a}\bar{x} = \bar{1} \Leftrightarrow ax = 1 + km \Rightarrow$ НОД$(a,m) = 1$.

2) Если НОД$(a,m) = 1$, то из алгоритма Евклида нахождения НОД(a,b) следует, что существуют x и y: $ax + my = 1 \Rightarrow \bar{a}\bar{x} = \bar{1}$ в $\mathbb{Z}/m\mathbb{Z}$.

Число натуральных числе, взаимно простых с m и меньших m, называется функцией Эйлера и обозначается $\varphi(m)$.

Задача 25. $(m,n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\cdot\varphi(n)$.

Задача 26. Вычислить $\varphi(p^n)$.

В $\mathbb{Z}/m\mathbb{Z}$ элементы, взаимно простые с m, образуют группу по умножению. Ее обычно обозначают $(\mathbb{Z}/m\mathbb{Z})^*$.

Лемма. Во всякой группе $G: |G| = n < \infty$, $\forall g\ g^n = e$. Это следствие т. Лагранжа.

Следствие. В $(\mathbb{Z}/m\mathbb{Z})^*$ $\forall a$: НОД $(a,m) = 1$ $\bar{a}^{\varphi(m)} = \bar{1} \Leftrightarrow a^{\varphi(m)} \equiv 1 \pmod m$.

Пример. $m = p$ – простое, $\varphi(m) = p-1$, $\forall n$: НОД$(n,p) = 1 \Rightarrow n^{p-1} \equiv 1 \pmod p$ или $n^p \equiv n \pmod p$. Это называется малой теоремой Ферма.

2. Лемма. /№/ Если конечная группа G действует на множестве M, то порядок всякой орбиты делит порядок группы или $|орб\ x| = [G : H_x]$, где $H_x = stab_G x$.

Рассмотрим, например, действие группы на себе сопряжением. e составляет отдельную орбиту. Орбиты наз. классами сопряженных элементов.

Пример. $G = S_3$ Орбиты составляют такие множества: $\{e\}$; $\{(12),(23),(13)\}$; $\{(123),(132)\}$.

Утверждение. $\tau = (ijk\dots)$. Тогда для всякого σ $\sigma\tau\sigma^{-1} = (\sigma(i)\,\sigma(j)\,\sigma(k)\dots)$

Для док-ва надо посмотреть, куда $\sigma\tau\sigma^{-1}$ переводит $\sigma(i), \sigma(j)\dots$

Следствие. Две подстановки τ_1 и τ_2 сопряжены в $S_n \Leftrightarrow$ в циклической записи они содержат одинаковое число циклов одинаковой длины.

Упражнение. Найти разбиение S_4 на классы сопряженных элементов.

3. $H \subset G$ – подгруппа. $H, g_1Hg_1^{-1}, \dots, g_kHg_k^{-1}$ – орбиты группы H. Что такое $stab_G(H) = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$? Это последнее равенство означает, что $N_G(H)$ – наибольшая подгруппа в G, содержащая H, и такая, что $H \lhd N_G(H)$.

Следствие. Число подгрупп, сопряженных с H, равно индексу нормализатора $[G : N_G(H)]$ и, в частности, делит порядок группы. ($N_G(H)$ – наз. нормализатором H в G.)

4. Напомним, $Z_G = \{x \in G \mid \forall g \in G \quad gxg^{-1} = x\}$ – центр группы G, т.е. центр состоит из тех элементов, которые при сопряжении составляют целую орбиту.

Задача 27. $A : G \to Aut\, G : A(g) = Ag$ (каждый элемент g переходит во внутренний автоморфизм, задаваемый этим элементом). $A(G) = Int\, G$. Д-ть, что $Ker\, A = Z_G$.

Следствие. $Z_G \triangleleft G$ и $Int\, G \simeq G/Z_G$.

Иногда удается из числовых соображений выяснить, является ли центр тривиальным или не является.

Теорема. $|G| = p^n \Rightarrow Z_G \neq \{e\}$.

Д-во. Рассмотрим орбиты сопряжения: $\{e\}, \{x_1, \dots, x_{p^k}\}, \{y_1, \dots, y_{p^k}\}, \dots$ Подсчитаем число элементов в G. $p^n = 1 + p^k + p^k + \dots$ По лемме 1 число элементов в орбите делит порядок группы. Приведенный расчет показывает, что помимо $\{e\}$ есть еще и другие орбиты, состоящие только из одного элемента. Они и составляют Z_G.

5. $G \triangleright N$ Каноническая проекция $G \xrightarrow{\psi} G/N$ отображает каждую подгруппу $H \subset G$ на подгруппу $\psi(H) = \bar{H} \subset G/N$. Для всякой $\bar{H} \subset G/N$ подгруппы в G/N рассмотрим $\psi^{-1}(\bar{H})$ – полный прообраз $\psi^{-1}(\bar{H}) = \{g \in G \mid \psi(g) \in \bar{H}\}$.

Утверждение. $\psi^{-1}(\bar{H})$ подгруппа в G. Вообще говоря, $\psi^{-1}(\psi(H))$ больше, чем H, т.к. $\psi^{-1}(\psi(H))$ со всяким $h \in H$ содержит и весь класс hN.

Обозначим $HN = \{hn \mid h \in H, n \in N\}$

Следствие. Если $N \triangleleft G$, то HN – подгруппа в G. Действительно, тогда $HN = \psi^{-1}(\psi(H))$ и $\psi(H) = HN/N$.

Посмотрим теперь на гомоморфизм ψ как на гомоморфизм, определенный только на H (обозначение $\psi|_H$ соответствует тому, что мы рассматриваем ψ, суженное на H). По теореме об эпиморфизмах $\psi(H) = H/Ker\, \psi|_H$, но $Ker\, \psi|_H = \{g \in H \mid \psi(g) = e\} = H \cap Ker\, \psi = H \cap N$. Итак, мы доказали

Теорему 1 (1-я об изоморфизме) $HN/N \simeq H/H \cap N$, где $N \triangleleft G$, а H – подгруппа в G. Кроме того мы установили тот факт, что $H = \psi^{-1}(\bar{H}) \Longleftrightarrow H \supset N$.

Утверждение. $\varphi : G_1 \to G_2$ эпиморфизм. Тогда φ^{-1} устанавливает биекцию между множеством подгрупп G_2 и множеством подгрупп G_1, содержащих $Ker\, \varphi$.

Примеры. 1. $H \subset S_n$ подгруппа. Если в H есть нечетные подстановки, то $H_+ = \{\sigma \in H \mid sgn\, \sigma = 1\} \triangleleft H$ и $H/H_+ \cong \mathbb{Z}/2\mathbb{Z}$.

Действительно, $H_+ = H \cap A_n$. $H/H_+ = H/H \cap A_n \simeq HA_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$, т.к. $HA_n = S_n$. (по условию в H есть нечетные подстановки.)

2. $V_4 \hookrightarrow S_4$ естественно вкладывается в S_4 и $V_4 \triangleleft S_4$ (Доказать.)

Задача 28. $S_3 \hookrightarrow S_4$. $S_3 = \{\sigma \in S_4 \mid \sigma(4) = 4\}$. Доказать, что $S_3 V_4 = S_4$.

Тогда $S_4/V_4 \simeq S_3V_4/V_4 \simeq S_3/S_3 \cap V_4 = S_3/\{e\} = S_3$

Теорема (2-я об изоморфизме) $G_1 \xrightarrow{\psi_1} G/N = G_2$, $H_2 \triangleleft G_2$, пусть $H_1 = \psi_1^{-1}(H_2)$. Тогда $H_1 \triangleleft G_1$ и $G_1/H_1 \simeq G_2/H_2$. (Другая формулировка: $G/N\,/H/N \simeq G/H$).

Док-во. Рассмотрим композицию гомоморфизмов: $G_1 \xrightarrow{\psi_1} G_1/N_1 = G_2 \xrightarrow{\psi_2} G_2/H_2 = G_3$

$\psi_2 \circ \psi_1 : G_1 \to G_3$ – гомоморфизм (проверьте). $Ker\, (\psi_2 \circ \psi_1) = H_1$ (проверьте). По теореме об эпиморфизме $G_2/H_2 \simeq G_3 \simeq G_1/H_1$, ч.тд.

Лекция 6. Глава 2. Кольца, поля.

§1. Определения, примеры, простейшие свойства.

Определение 1. Кольцом K наз. множество с двумя операциями $+, \cdot$. K – абелева группа по сложению $(+)$, операция $\cdot$ ассоциативна и дистрибутивна, т.е.

3а. $(a + b) \cdot c = a \cdot c + b \cdot c$

3б. $a \cdot (b + c) = ab + ac$ (знак $\cdot$ часто опускается).

Примеры: 1) $\mathbb{Z}$; 2) $\mathbb{Z}/m\mathbb{Z}$; 3) $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$; 4) $Mat_n\begin{pmatrix}\mathbb{Z}\\ \mathbb{Q}\\ \mathbb{R}\end{pmatrix}$
5) кольца функций $\mathcal{F}(X,K) = \{f : X \to K$, где K – кольцо$\}$.

Замечание. 1) Если $ab = ba$, то K наз. коммутативным кольцом.
2) Если в K существует 1: $1a = a1 = a$ $\forall a \in K$, то K наз. кольцом с единицей.

Свойства. 1) $a0 = 0a = 0$; 2) $a\cdot(-b) = (-a)\cdot b = -ab$; 3) $a - b =$ (по определению) $= a + (-b)$, аналогично $(a-b)c = ac - bc$, $a(b-c) = ab - ac$; 4) из ассоциативности сложения следует, что определена всякая конечная сумма $a_1+a_2+\ldots+a_n = \sum_{k=1}^{n} a_k$; Из ассоциативности умножения вытекает, что определено любое конечное произведение $a_1a_2\ldots a_n = \prod_{k=1}^{n} a_k$; 5) делители нуля: например, в $\mathbb{Z}/4\mathbb{Z}$ $\bar{2}\cdot\bar{2} = \bar{4} = \bar{0}$. Определение. $a_0 \in K$ наз. левым делителем нуля, если $\exists$ $b \neq 0$: $ab=0$, аналогично, правым делителем нуля наз. такой $0 \neq b \in K$, что найдется $a \neq 0$ из K, для которого $ab = 0$.

Упражнение. а) в $\mathbb{Z}$ нет делителей 0; в) привести примеры делителей 0 в кольцах $Mat_n(\cdot)$ и кольце функций (операция – умножение)

Определение. Полем F наз. мн-во с двумя операциями $+,\cdot$, причем F – абелева группа по сложению, $F\setminus\{0\}$ (по определению F^*) – абелева группа по $\cdot$, и справедливы два естественных закона дистрибутивности.

Замечание. Другими словами, поле – это коммутативное кольцо с единицей, в котором всякий элемент $a \neq 0$ имеет обратный a^{-1}.

Примеры. 1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$; 2) $F_p = \mathbb{Z}/p\mathbb{Z}$, где p – простое; 3) $F_4 = \{0, 1, i, 1+i\}$ причем $i^2 = 1 + i$ (чему равно $(1+i)^2$?)

Еще примеры колец: $F_p[x]$, $Mat_2(F_2)$.

Упражнение. Сколько многочленов степени, не больше 2 в $F_p[x]$?

Замечание. В конечных полях различны понятия многочлена и функции. Функций мало.

Определение. Элемент кольца K a наз. обратимым или единицей K (с единицей), если для него существует a^{-1}: $a\cdot a^{-1} = 1$.

Задача 29. Есть ли единицы в $F_2[x]$, степени $deg \leq 2$?

Задача 30. Найти все делители 0 степени ≤ 2 в $F_2[x]$.

Определение. K – кольцо с операциями $(+,\cdot)$. $K_1 \subset K$ наз. подкольцом, если K_1 само есть кольцо относительно тех же операций. Это значит, что K_1 – подгруппа по сложению и для всяких $a,b \in K_1 \Rightarrow ab \in K_1$.

Если F – поле с операциями $(+,\cdot)$. Так же определяется подполе $F_1 \subset F$. В этой ситуации еще говорят, что F является расширением поля F_1. Эта терминология имеет важное психологическое и историческое значение, т.к. $\mathbb{R}$ и $\mathbb{C}$ получились последовательным расширением $\mathbb{Q}$.

Точно так же, как и в группах определяется гомоморфизм (или просто морфизм) колец, полей.

Определение. $\varphi : K_1 \to K_2$ наз. морфизмом колец, если $\forall$ a,b K_1 $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\cdot\varphi(b)$.

$\varphi : F_1 \to F_2$ наз. морфизмом полей, если $\forall$ $a,b \in F_1$ выполняются те же св-ва

Так же определяются эпи, моно и изоморфизмы колец, полей.

Попытаемся теперь классифицировать гомоморфизмы.

1) $\varphi : K_1 \to K_2$ морфизм колец. φ раскладывается в композицию $K_1 \xrightarrow[\text{эпи}]{\varphi} \varphi(K_1) \xhookrightarrow[\text{моно}]{} K_2$

Лемма $\varphi(K_1)$ – подкольцо в K_2.

Пусть теперь $\varphi : K_1 \to K_2$ эпиморфизм, забудем пока об операции $\cdot$ в K_1 и K_2 $K_1 \xrightarrow{\varphi} K_2$ эпиморфизм групп $(+)$ и $\mathcal{J} = Ker\,\varphi = \{k \in K_1 \mid \varphi(k) = 0\}$. Тогда по теореме об эпиморфизме групп $K_1 \xrightarrow{\varphi} K_2$ K_2 и $K_1/\mathcal{J}$ изоморфны, как группы

$\psi \to K_1/\mathcal{J}$

по сложению. Можно ли в $K_I/\mathcal{J}$ ввести умножение так, чтобы $K_2 \tilde{=} K_I/\mathcal{J}$ был бы изоморфизмом, а ψ – эпиморфизмом колец? $\psi: a \mapsto a+\mathcal{J}$; $\psi: в \mapsto в+\mathcal{J}$; $\psi: ав \mapsto (a+\mathcal{J})(в+\mathcal{J}) = ав + a\mathcal{J} + \mathcal{J}в + \mathcal{J}^2$. Чтобы ψ был эпиморфизмом колец, нужно, чтобы $a\mathcal{J} + \mathcal{J}в + \mathcal{J}^2 \subset \mathcal{J}$

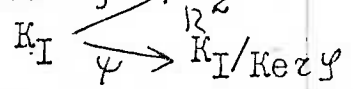
Определение. $\mathcal{J} \subset K$ наз. двусторонним идеалом, если I) $\mathcal{J}$ – подкольцо и
2) $\forall a \in K$ $a\mathcal{J} \subset \mathcal{J}$ и $\mathcal{J}a \subset \mathcal{J}$.

Пример. $K = \mathbb{Z}$, $\mathcal{J} = 2\mathbb{Z}$ – идеал (двусторонний идеал обычно именуется просто идеалом).

Утверждение. $\varphi: K_I \to K_2$ – морфизм колец. Тогда $\mathcal{J} = \operatorname{Ke}\varphi$ – идеал.

Док-во. Пусть $a \in \mathcal{J}$, $в \in K$. Рассмотрим ав. $\varphi(ав) = \varphi(a)\cdot\varphi(в) = 0\cdot\varphi(в) = 0$, т.е. $ав \in \mathcal{J}$. Так же доказывается "поглощаемость" с другой стороны. Всё.

Теорема. (об эпиморфизме колец) $\varphi: K_I \to K_2$ – эпиморфизм. Тогда следующая диаграмма коммутативна:



Итак, всякий гомоморфизм есть каноническая проекция на фактор-кольцо по идеалу.

Пример. I. $\mathbb{Z}/m\mathbb{Z}$ – оправданное обозначение для колец.
2. Для полей ситуация в корне другая.

Теорема. Пусть $\varphi: F_I - F_2$ – морфизм полей. Тогда либо φ – моно, либо $\varphi(F_I) = 0$.

Док-во. $\varphi: F_I - F_2$ – гомоморфизм групп по сложению. Пусть найдется $x \neq 0$, такой, что $\varphi(x) = 0$. Тогда а) $\varphi(I) = \varphi(xx^{-I}) = \varphi(x)\cdot\varphi(x^{-I}) = 0\cdot\varphi(x^{-I}) = 0$.
б) $\forall y \in F_I$ выполнено $\varphi(y) = \varphi(Iy) = \varphi(I)\cdot\varphi(y) = 0\cdot\varphi(y) = 0$, ч.т.д.

Лекция-семинар.

Утверждения (задачи).

I) Пересечение подколец (подполей) – подкольцо (подполе).
2) Пересечение идеалов – идеал.
3) Если $K_I \subset K$ – подкольцо, $\mathcal{J} \lhd K$ ($\mathcal{J}$ идеал в К), то $K_I \cap \mathcal{J} \lhd K_I$ ($K_I \cap \mathcal{J}$ идеал в K_I).
4) Теоремы о соответствии подколец (идеалов) при эпиморфизмах колец.
Пусть $\varphi: K \to K_I$ эпиморфизм колец, $\mathcal{J}_0 = \operatorname{Ke}\varphi$, $M = \{\mathcal{J} \lhd K \mid \mathcal{J} \supset \mathcal{J}_0\}$; $M_I = \{\mathcal{J} \lhd K_I$, $\mathcal{J}$ – любое$\}$; $N = \{K_2 \subset K \mid K_2$ – подкольцо и $\mathcal{J}_0 \subset K_2\}$; $N_I = \{K_2 \subset K_I \mid K_2$ подкольцо$\}$.

Теоремы формулируются так: существует биекция между множествами M и M_I (N и N_I) и эту биекцию устанавливает функция φ^{-I} (полный прообраз).

5) К – кольцо, $\mathcal{J} \lhd K$, $L \subset K$ – подкольцо $\{L, \mathcal{J}\} = \{l + j \mid l \in L, j \in \mathcal{J}\}$.
Тогда $\{L, \mathcal{J}\}/\mathcal{J} \cong L/L \cap \mathcal{J}$

Теорема. Всякое кольцо К вкладывается в кольцо $K^{ж}$ с единицей.

Идея очень проста: присоединить к элементам кольца I и постараться доопределить умножение; введем обозначения: $\underbrace{к+к+\ldots+к}_{п} = пк$; $\underbrace{I+I+\ldots+I}_{м} = мI = м$;
$(м+к)\cdot(п+р) = мп+мр+кп+кр$.

Док-во лучше дать конструкцией $K^{ж} = \mathbb{Z} \oplus K = \{(м,x) \mid м \in \mathbb{Z}, x \in K\}$ (прямая сумма, как абелевых групп); $(м_1,x_1)+(м_2,x_2) = (м_1+м_2, x_1+x_2)$. Определим теперь умножение так: $(м,x)\cdot(п,y) = (мп, му+пх+xy)$. Свойства кольца проверяются.

$K \overset{\varphi}{\hookrightarrow} K^{ж}$ $\varphi: к \mapsto (0,к)$, $e = (I,0)$.

Следствия. I) К – коммутативно $\Rightarrow K^{ж}$ – коммутативно.

Пример. А – абелева группа. $End\,A = \{\varphi: A \to A$ – гомоморфизмы$\}$. $End\,A$ – кольцо с единицей. $(g+f)(x) = g(x) + f(x)$, $(g\circ f)(x) = g(f(x))$, $e = id_A$
$End\,\mathbb{Z} = \mathbb{Z}$; $End\,\mathbb{Q} = \mathbb{Q}$.

Задача. Найти $End\,\mathbb{Z}/n\mathbb{Z}$

Теорема. Всякое кольцо К с правой единицей может быть мономорфно вложено

в кольцо $\mathrm{End}_{\mathbb{Z}} A$, где A – абелева группа.
Док-во. В качестве A возьмем аддитивную группу кольца K (обозначение: $K_{адд}$). Она абелева по определению. Для всякого $k \in K$ $\lambda_k : K_{адд} \to K_{адд}$ определим естественно $\lambda_k(x) = kx$. Все свойства проверяются непосредственно.

Лекция 8.
Пусть K – кольцо с единицей, $\mathcal{T}_0$ – идеал K; $K/\mathcal{T}_0$ – опять кольцо. Вопрос: когда $K/\mathcal{T}_0$ – поле? Сопоставим два факта а) теорему о морфизме полей и б) теорему о соответствии идеалов при эпиморфизме колец. Из а) следует, что в полях нет собственных идеалов, кроме $\{0\}$ – нулевого.
Задача. $K \rhd \mathcal{T}$, в $\mathcal{T}$ нет обратимых элементов, с другой стороны, если $\mathcal{T}_0 \subset \mathcal{T}$, то $\mathcal{T}/\mathcal{T}_0$ идеал в $K/\mathcal{T}_0$.
Определение. $\mathcal{T} \lhd K$ наз. максимальным (мах), если он не содержится ни в каком другом идеале (из $\mathcal{T}_1 \supset \mathcal{T} \Rightarrow \mathcal{T}_1 = \mathcal{T}$).
Теорема. K – коммутативное кольцо с единицей; $\mathcal{T} \lhd K$. $K/\mathcal{T}$ – поле $\Longleftrightarrow \mathcal{T}$ – мах
Эту теорему мы уже фактически доказали. Пусть $0 \neq m \in K/\mathcal{T} = K_I$ не обратим. Рассмотрим $mK_I = \mathcal{T}_I$ – это идеал в K_I (проверьте!). $I \notin K_I$, т.к. m не обратим $\Rightarrow \mathcal{T}$ не мах. Остальные аксиомы проверяются непосредственно.

Идеал aK наз. главным идеалом.
Задача. $m\mathbb{Z}$ – мах $\Longleftrightarrow$ m – простое.
Следствие. $\mathbb{Z}/m\mathbb{Z}$ поле $\Longleftrightarrow m = p$ – простое.
Отступление. $\mathrm{char}\, F$ – характеристика поля. Рассмотрим поле F, его аддитивную группу и такое множество: 1_F, $1_F + 1_F$, ..., $m1_F$, ... Возможны два случая:
а) В этом ряду все элементы не нулевые. В таком случае говорят, что $\mathrm{char}\, F$ равна 0.
Следствие: во всяком поле нулевой характеристики есть подполе, изоморфное полю рациональных чисел. ($F \supset F_I \simeq \mathbb{Q}$)
Действительно, определим $\varphi : \mathbb{Q} \to F$ следующим образом. $\varphi(1) = 1_F$, тогда $\varphi(m) = \varphi(m1) = \varphi(1+1+\ldots+1) = \varphi(1) + \varphi(1) + \ldots + \varphi(1) = m \cdot 1_F$. Положим $1_F/n$ равным ℓ: $\ell \cdot (n1_F) = 1_F$. $\varphi(1/n) = 1_F/n \Rightarrow \varphi(m/n) = (m/n) \cdot 1_F$. Все доказано.
б) Найдется m такое, что $m1_F = 0_F$.
Определение. Наименьшее m: $m1_F = 0_F$ наз. $\mathrm{char}\, F$.
Лемма. $\mathrm{char}\, F$ – простое число. Док-во. Пусть $m = nk$. $m1_F = (n1_F) \cdot (k1_F) = 0$, но m – наименьшее, делителей 0 нет $\Rightarrow$ m – простое.
Следствие. Если $\mathrm{char}\, F = p$, то найдется подполе $\simeq F_p$. Д-во. Построим $\varphi : F_p \to F$ так: $\varphi(1_{F_p}) = 1_F$. Остальное стандартно.
Указание к задаче о мах иделае вида $m\mathbb{Z}$. Докажите сперва, что в $\mathbb{Z}$ любой идеал главный.
Пример. $K = \mathbb{Z}$ и $m\mathbb{Z}$, где $m = 2, 3, 4, 6, 12$.
Теорема. Если K – кольцо с единицей, то всякий идеал $\mathcal{T}_0$ в K содержится в некотором мах. идеале $\mathcal{T}_{max}$.
Док-во. 1. Условимся, что мы будем рассматривать только собственные идеалы, в поле это означает, что $0 \neq 1$.
2. $1 \notin \mathcal{T}_0$. 3. $\mathcal{T}_0$ либо мах, либо нет, $\mathcal{T}_1 \supset \mathcal{T}_0$ либо мах, либо нет. Пусть $\mathcal{T}_0 \subset \mathcal{T}_1 \subset \mathcal{T}_2 \subset \ldots \subset \mathcal{T}_k \subset \ldots$ и $\mathcal{T}^* = \bigcup_{k=1} \mathcal{T}_k$ тогда $\mathcal{T}^*$ – идеал (проверьте!), причем: а) не содержит 1: $\mathcal{T}^* \not\ni 1$; б) $\mathcal{T}^* \supset \mathcal{T}_0$ в) является ли $\mathcal{T}^*$ мах? Вообще говоря, нет.
Пример: $\mathcal{F}(X,F) = \{ f : X \to F \mid X$ – мн-во, F – поле$\}$ /например, $F = \mathbb{R}$/.
$Y \subset X$ $\mathcal{T}_Y = \{ f \in \mathcal{F}(X,F) \mid f(y) = 0 \ \forall y \in Y \}$. $\mathcal{T}_{Y_1} \subset \mathcal{T}_{Y_2} \Longleftrightarrow Y_1 \supset Y_2$. $\mathcal{T}_{max} \Longleftrightarrow$
$\Longleftrightarrow \mathcal{T} = \mathcal{T}_{x_0}$

Вернемся к примеру с функциями. $\mathcal{J}_{max} = \mathcal{J}_{x_0} = \{f \in \mathcal{F}(X,F) \mid f(x_0) = 0\}$. $\mathcal{F}(X,F)/\mathcal{J}_{x_0} \simeq F \triangleleft \varphi_{x_0}: \mathcal{F}(X,F) \to F$ $\varphi_{x_0}(f) = f_{x_0}$ – это морфизм колец. $\operatorname{Ker}\varphi_0 = \mathcal{J}_{x_0}$ и по теореме об эпиморфизме получаем нужный изоморфизм. ▸

Пусть $F = \mathbb{R}$; $X = [a,b]$; $\mathcal{J}_0 = \mathcal{J}_{[c_0,d_0]}$

Рассмотрим ... $\subset [c_2,d_2] \subset [c_1,d_1] \subset [c_0,d_0]$. $\mathcal{J}^* = \cup \mathcal{J}_{[c_i,d_i]} = \mathcal{J}_{\cap [c_i,d_i]}$, Но $\cap [c_i,d_i] \neq \{x_0\}$ не обязательно. Опять приходится пользоваться услугами теории множеств. Отступление. Упорядоченные множества. См. Ван дер Варден, Алгебра, глава 7.

Лекция 9.

§ 3. Целостные кольца

Определение 1. Целостным кольцом (= кольцо целостности, область целостности) называется коммутативное кольцо без делителей 0 с единицей.

Примеры. 1) $\mathbb{Z}$; 2) Любое поле F; 3) K[x], где K – целостное кольцо.

Теорема. Любое целостное кольцо мономорфно вложимо в поле F, т.е. существует наименьшее поле F и $\varphi: K \to F$ – вложение.

Д-во. Провести самим, вспомнив построение $\mathbb{Q}$ из $\mathbb{Z}$.

то поле называется полем частных кольца K и обозначается Q(K)./$\mathbb{Q} = Q(\mathbb{Z})$/.

Определение 2. Для любого множества $M \subset K$ и любого $a \in K$ $aM = \{am \mid m \in M\}$.

В кольце K множество aK называется главным идеалом, порожденным эл-том a (короче: главный идеал эл-та a).

Упражнение. Проверить, что aK идеал в K. /aK обозначается еще (a)/.

Целостное кольцо, любой идеал которого главный, наз. кольцом главных идеалов.

Примеры. 1) $\mathbb{Z}$; 2) любое поле F; 3) F[x], где F – поле.

Упражнение: Доказать, что F[x] – кольцо главных идеалов.

§ 4. Теория делимости в целостных кольцах

В этом параграфе K обозначает целостное кольцо. $K^* = K \setminus \{0\}$.

Определение. $a \vdots b \Longleftrightarrow b \mid a$ (говорят, что a делится на b или b делит a), если $\exists\, c$: $a = bc$.

Упражнение: доказать, что если $b \mid a$, то c единственно.

Определение Обратимые элементы в целостном кольце наз. делителями единицы.

Упражнение Делители единицы K образуют группу по умножению.

Если $b \mid a$, и $\varepsilon \mid 1$, то $\varepsilon b \mid a$. εb называют делителем, ассоциированным с элементом a (или, короче, ассоциированным делителем)

Упражнение. Отношение ассоциированности есть отношение эквивалентности.

Лемма 1. $a \mid 1 \Longleftrightarrow (a) = K$. Лемма 2. $a \mid b \Longleftrightarrow (a) \supset (b)$.

Определение Для всякого эл-та a делители, ассоциированные с 1 и с a наз. тривиальными делителями, все остальные – наз. собственными.

Лемма 3. a – собственный делитель $b \Longleftrightarrow (a) \supset (b)$, и $(a) \neq (b)$.

Лемма 4. $a \mid b$ и $b \mid 1 \Rightarrow a \mid 1$.

Определение $a \in K^*$ наз. простым (в некоторых кольцах – неприводимым), если он обладает только тривиальными делителями.

Лемма 5. K – кольцо главных идеалов. $a \in K$ прост $\Longleftrightarrow$ (a) – мах /идеал (a) – максимальный).

Определение $a, b \in K$. НОД (a,b) наз. элемент c, такой что $c \mid a$, $c \mid b$ и из ($d \mid a$, $d \mid b$) $\Rightarrow d \mid c$. c определен с точностью до ассоциированности.

Теорема. Пусть K – кольцо главных идеалов. Для $\forall\, a, b \in K$ $\exists$ c = НОД (a,b).

Д-во. Положим $\mathcal{J} = \{\alpha a + \beta b \mid \alpha, \beta \in K\}$. Тогда 1) $\mathcal{J}$ – идеал; 2) $\mathcal{J} \supset (a), (b)$. Т.к. K – кольцо главных идеалов $\Rightarrow \exists c$: $\mathcal{J} = (c) \Rightarrow c \mid a$ и $c \mid b$. При этом $c = \alpha a + \beta b$ для некоторых $\alpha, \beta \in K$. Пусть $d \in K$ так, что $d \mid a$ и $d \mid b \Longleftrightarrow a = dm_1$,

$в = dm_2$, $с = \alpha d m_1 + \beta d m_2 = d(\alpha m_1 + \beta m_2) \Rightarrow d \mid с$, т.е. с= НОД (а,в), ч.т.д.

Замечание. Идеал $\mathcal{T}$ можно было определить, как (а)$\cap$(в), но тогда нужно доказывать, что НОД (а,в) $= \alpha а + \beta в$ для некоторых $\alpha, \beta \in К$. Это св-во НОД нам когда-нибудь понадобится.

Определение. а,в$\in$К наз. взаимно простыми, если НОД (а,в) = I.

Лемма 6. Пусть $р \in К$ - простой и $р \mid а = в_I в_2 \ldots в_к$, К - кольцо главных идеалов. Тогда $\exists\, i$: $р \mid в_i$. Док-во. индукцией по к. I^0. очевидно. 2^0. Проведем для $а = в_I в_2$. Возможны два случая: а) $р \mid в_I$ - все доказано. б) $р \nmid в_I \Rightarrow$ р и $в_I$ взаимно просты. $\Rightarrow I = в_I м + рп$. Умножим это рав-во на $в_2$. $в_2 = в_I в_2 м + рпв_2 \Rightarrow$ $в_2 = ам + рпв_2 \Rightarrow в_2 = ра_I м + рпв_2$, т.к. $р \mid а$. Последнее рав-во означает, что $р \mid в_2$.

Определение. Кольцом с однозначным разложением на простые множители (короче, факториальным кольцом, гауссовым кольцом) наз. целостное кольцо К со свв-вами: для $\forall а \neq 0$: 1) $а = u\, р_I \ldots р_к$, где $u \mid I$, $р_i$ - простые, к - конечно; 2) Если есть два таких разложения $а = u\, р_I р_2 \ldots р_к$ и $а = v q_1 q_2 \ldots q_s$, то $к = s$ и $q_1 = u_1 р_{i_1}$; $q_2 = u_2 р_{i_2}$; ... где $u_i \mid 1$. (эти два свойства выражают "однозначное разложение на простые множители")

Теорема I. Кольцо главных идеалов факториально.

Д-во. I. $(а) \subset \mathcal{T}_{мах}$ (любой идеал содержится в максимальном). К - кольцо главных идеалов $\Rightarrow \mathcal{T}_{мах} = (р_I)$, по лемме 5 $р_I$ - прост $\Rightarrow а = р_I а_I$; проделаем то же с $а_I$ и т.д. Докажем, что этот процесс кончится. Рассмотрим $(а) \subset (а_I) \subset \ldots$ $\mathcal{T} = \bigcup\limits_к (а_к)$ - идеал в К $\Rightarrow \mathcal{T} = (в)$, но элемент $в \in \bigcup\limits_к (а_к) \Rightarrow в \in (а_s)$ при некотором $s \Rightarrow (а_s) = (а_{s+1}) = \ldots$ и $(а_s) = (в)$, $в = р_s$ - прост.

2. Пусть есть два разложения. $а = u р_1 р_2 \ldots р_r$ и $а = v q_1 q_2 \ldots q_s$; $р_i, q_j$ - простые, рассмотрим q_1 : $q_1 \mid а = u р_1 \ldots р_r$, по лемме 6 $q_1 \mid р_{i_1} \Rightarrow$ (из простоты $р_i$) $q_1 = u_1 р_{i_1}$ и т.д.

Определение К - целостное кольцо наз. евклидовым кольцом, если $\exists\, \delta : К^* \to \mathbb{N} \cup \{0\}$ (будем называть δ - степенью а) со свойствами: I) $\delta(ав) \geq \delta(а)$; 2) $\forall\, а, в \in К$ $в \neq 0$ $\exists\, q, r \in К$ (q - "частное", r - "остаток"): $а = qв + r$ и ($\delta(r) < \delta(в)$ или $r = 0$). Примеры. I. $\mathbb{Z}$ с $\delta(а) = |а|$; 2) F[x] $\delta(р(х)) = \deg р(х)$ - степень многочлена.

Замечание. Св-во 2) в определении степени δ означает, что в кольце К осуществим алгоритм Евклида деления с остатком.

Теорема 2. Всякое евклидово кольцо К является кольцом главных идеалов.

Д-во. Пусть $\mathcal{T} \lhd$ К - идеал в К. Рассмотрим в $\mathcal{T}$ элемент в, такой что $\delta(в) = \min\limits_{с \in \mathcal{T}} \delta(с)$, т.е. в - эл-т с минимальной степенью. Утверждается, что $\mathcal{T} = (в)$. Возьмем $\forall\, а \in \mathcal{T}$, для пары (а,в) $\exists\, q, r$: $а = qв + r$ либо $\delta(r) < \delta(в)$, что противоречит выбору в (почему $r \in \mathcal{T}$?) - либо $r = 0 \Rightarrow а \in (в)$.

Следствие. I) $\mathbb{Z}$ - евклидово $\Rightarrow \mathbb{Z}$ - кольцо главных идеалов $\Rightarrow \mathbb{Z}$ - факториально. Теорема I для $\mathbb{Z}$ наз. основной теоремой арифметики.

2) F[x] - евклидово $\Rightarrow$ F[x] - кольцо главных идеалов (всякий идеал в F[x] имеет вид $р(х) \cdot F[x]$) $\Rightarrow$ F[x] факториально. Простые элементы в F[x] наз. неприводимыми многочленами.

Задача. Найти все неприводимые многочлены в $\mathbb{R}[x]$.

Лекция I0.

Теоремы I и 2 предыдущей лекции обозначают, что имеют место такие включения: {евклидовы кольца} $\subset$ {кольца главных идеалов} $\subset$ {факториальные кольца}. На самом деле эти включения точные.

Примеры: I) Кольцо F[X,У] многочленов от двух переменных не является кольцом главных идеалов. Рассмотрим множество многочленов в нем с нулевым свободным членом. Это мн-во - идеал $\mathcal{T}$ (докажите!), но данный идеал не является главным. Докажите это. (Указание: $х \in \mathcal{T}$ и $у \in \mathcal{T}$).

Задача. F[X,У] - факториально. Задача. Придумать пример (или найти где-нибудь) кольца главных идеалов, не являющиеся евклидовыми.

2) Не всякое целостное кольцо факториально. Рассмотрим $\mathbb{Z}[\sqrt{-3}] = \{м + п\sqrt{-3} \mid м, п \in \mathbb{Z}\}$. $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Q}(\sqrt{-3})$. $\mathbb{Q}(\sqrt{-3})$ – поле, следовательно, $\mathbb{Z}[\sqrt{-3}]$ – кольцо целостности. В $\mathbb{Z}[\sqrt{-3}]$ есть норма $N : \mathbb{Z}[\sqrt{-3}] \to \mathbb{N} : N(м + п\sqrt{-3}) \overset{def}{=} (м^2 + 3п^2)$. $N(ав) = N(а)N(в)$ /проверьте!); $N(1) = 1$, $N(a^{-1}) = N(a)^{-1} \Rightarrow N(a) = 1 \Leftrightarrow a = \pm 1$ – делители 1. Разложение на простые множители в $\mathbb{Z}[\sqrt{-3}]$ возможно (докажите), но оно на единственно! Пример: $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$. /Докажите, что 2 и $1 \pm \sqrt{-3}$ – простые./ (См. Кострикин, стр. 223).

В евклидовом кольце для любых a и $в \in К$ $(в \neq 0)$ $а = q_1 в + r_1$, $\delta(r_1) < \delta(в)$; $в = q_2 r_1 + r_2$; $\delta(r_2) < \delta(r_1)$; ... т.к. $\delta(u) \in \mathbb{N} \cup \{0\}$, то $\exists k \in \mathbb{N}$: $r_{k-2} = q_k r_{k-1} + r_k$; $r_{k-1} = q_{k+1} \cdot r_k$, $r_{k+1} = 0$.

Лемма 1. r_k = НОД (а,в) Эта лемма позволяет находить НОД для любых (а,в) в евклидовых кольцах.

Упражнение найти НОД (411193635, 128001)

В кольцах главных идеалов для любых а,в $К^{*}$ $\exists \alpha, \beta$: НОД(а,в) $= а\alpha + в\beta$. Алгоритм Эвклида в евклидовых кольцах позволяет находить α, β для любых а,в.

Упражнение. Найти α и β для а и в из предыдущего упражнения.

Такая пара α и β не единственная. НОД(а,в) $= а\alpha + в\beta = а(\alpha + в) + в(\beta - а)$.

Задача. В евклидовых кольцах К для $\forall$ $а, в \neq 0$ $\exists !$ α, β такие, что НОД(а,в) $= а\alpha + в\beta$ и $\delta(\alpha) \leq \delta(в)$, $\delta(\beta) \leq (\alpha)$.

Упражнения к §3 и §4.

1. $К \subset F \Rightarrow К$ – целостное кольцо.
2. $\mathbb{Z}[X]$ – факториально.
3. $\mathbb{Z}[X] \supset \mathcal{T} = \{ f(x) = a_n x^n + \ldots + a_1 x + a_0 \mid (2 \mid a_k) \}$ $\mathcal{T}$ не является главным идеалом. Задачи 2. и 3. показывают, что включение {кольца главных идеалов} $\subset$ {факториальные кольца} – строгое.
4. Доказать, что ненулевой элемент р факториального кольца К прост $\Leftrightarrow$ К/рК – целостное кольцо.
5. Если целостное кольцо К не поле, то К[X] – не кольцо главных идеалов.
6. Если целостное кольцо $К \subset F$ – поле и $\forall$ $f \in F$ $f = а/в$, то $F = \mathbb{Q}(К)$.
7. $\mathbb{Q}(\sqrt{\alpha}) = \mathbb{Q}(\mathbb{Z}[\sqrt{\alpha}])$.
8. Найти НОД $(x^5 + x^4 + 1,\ x^6 + x^5 - 6x^4 - 7x^3 - x^2 + 6x + 6)$.
9. Есть ли общие корни у следующих уравнений? $x^3 - 3x^2 - 3x - 4 = 0$ и $x^5 - 5x^4 + 9x^3 - 18x^2 - 7x - 4 = 0$.
10. $P(x) = x^3 + ax + в$. Найти все а,в, при которых P(x) имеет кратный корень (м. б., комплексный).
11. $P(x) = x^4 + ax^2 + вx + с$. Тот же вопрос.
12. Будет ли кольцо многочленов над $\mathbb{F}_p$ целостным?
13. Разложить на множители в $\mathbb{Z}[x]$, $\mathbb{R}[x]$ и $\mathbb{C}[x]$ $x^4 + 1$, $x^4 + 4$.
14. $\mathbb{Q}(A) \cong A \Leftrightarrow A$ – поле.

§ 5. Кольцо многочленов и поле отношений.

Рассмотрим кольцо многочленов над полем F $F[X]$. Напомним, что если F – конечное поле, то F[X] не совпадает с кольцом функций на F (вспомнить пример).

$F[X]$ – евклидово кольцо, $\delta(f) = \deg f$ – степень многочлена.

Делителями единицы в $F[X]$ являются эл-ты $F^{*} = F \setminus \{0\}$ – обратимые элементы поля F и только они. Простые элементы в $F[X]$ наз. неприводимыми многочленами. Поле частных кольца $F[X]$ $\mathbb{Q}(F[X])$ обозначается символом $F(X)$ /смена квадратных скобок на круглые./ и называется полем рациональных дробей от переменной X с коэффициентами в F.

Определение. Дробь f/g наз. несократимой, если НОД $(f, g) = 1$. f/g наз. правильной если $\deg f < \deg g$. Определим $\deg(f/g) = \deg f - \deg g$. Это число не зависит от представления дроби, т.к. $\deg(f \cdot g) = \deg f + \deg g$. Условимся, что $\deg 0 = -\infty$ (это удобно).

Лемма 1. Каждая рац. дробь f/g из $F(X)$ однозначно представляется в виде суммы многочлена и правильной дроби.

Док-во. Рассмотреть q и r для f и g из алгоритма Евклида.

Определение. Правильная рациональная дробь $f/g \in F(X)$ наз. простейшей, если $g = p^n$, $n \geq 1$, $p = p(x)$ – неприводимый многочлен и $\deg f < \deg p$.

Основной теоремой о рациональных дробях является

Теорема 1. Каждая правильная рациональная дробь f/g может быть разложена

единственным образом в сумму простейших. (Д-во см. Кострикин, стр.238–241)

Задача. Сформулировать и доказать подобное утверждение для поля $\mathbb{Q} = \mathbb{Q}(\mathbb{Z})$.

Задача. а) Поделить x^5+x^3+x+1 на x^2+2x-1 в $\mathbb{F}_3[X]$ с остатком.

б) То же самое в $\mathbb{F}_2[X]$

Задача. Вывести формулы $(x+y)^2$ в $\mathbb{F}_2[X,Y]$; $(x+1)^3$ в $\mathbb{F}_3[x]$; $(x+y)^p$ в $\mathbb{F}_p[X,Y]$.

§ 6. Расширения полей. Алгебраическое замыкание

Теорема (о существовании корня). Пусть $p(x) \in F[X]$ – неприводимый многочлен. Тогда существует расширение поля F – поле F_1 ($F_1 \supset F$) такое, что в F_1 есть корень многчлена $p(x)$.

Д-во. Рассмотрим $F_1 = F[X]/(p(x))$. Это поле (докажите!). Обозначим $(p(x)) = \mathcal{J}$ и $\pi: F[X] \to F[X]/\mathcal{J}$ – естественная проекция (кольцевой гомоморфизм). $F \subset F[X] \Rightarrow \pi: F \to F_1$ вложение, и можно для элементов $a \in F$ $\pi(a)$ отождествить с a. Пусть $p(x) = a_n x^n + \ldots + a_0$. Этот многочлен можно рассматривать как многочлен в в $F_1[x]$. Корнем многочлена $p(x)$ в $F_1[x]$ будет $\pi(X)$, где $X \in F[X]$. Действительно, $a_n \pi(X)^n + a_{n-1}\pi(X)^{n-1} + \ldots + a_0 = \pi(a_n)\cdot\pi(X^n) + \ldots + \pi(a_0) = \pi(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0) = \pi(p(X)) = 0$. всё.

Лекция II. Отступление I. $\mathbb{C}$.

$F = \mathbb{R}$, $p(x) = x^2+1$ – неприводимый мн-н. (Д-ть это.) $F_1 = F[X]/(x^2+1)$. Как устроено F_1? Пусть $(x^2+1) = \mathcal{J}$. Для всякого многочлена $f(x) \in F[X]$ в классе $f(x) + \mathcal{J}$ есть линейный многочлен. Действительно, $f(x) = q(x)(x^2+1) + r(x)$, причем $\deg r(x) < \deg(x^2+1) = 2$. $\Rightarrow r(x) = a + bx$. Рассмотрим класс $x + \mathcal{J}$. $(x+\mathcal{J})^2 = x^2 + \mathcal{J} = -1 + \mathcal{J}$. Это означает, что класс $x + \mathcal{J}$ является корнем многочлнеа x^2+1. "Но не поле F_1 называется полем комплексных чисел, а некий изоморфный ему объект, элементы которого изображаются точками плоскости." (Кострикин, стр.196, I абзац.)

$\mathbb{C} = \{a + bi \mid a,b \in \mathbb{R},\ i^2 = -1\}$, $z = a + bi$ изображается точкой на плоскости $\mathbb{C}$ координатами (a,b). $a = \mathrm{Re}\, z$ – вещественная часть z, а $b = \mathrm{Im}\, z$ – мнимая часть z. Элементы $a = a + 0\cdot i$ отождествляются с действительными числами $\mathbb{C}$. Действия: $a_1 + b_1 i + a_2 + b_2 i = (a_1+a_2) + (b_1+b_2)i$; $1 = 1 + 0\cdot i$.
$(a_1 + b_1 i)(a_2 + b_2 i) = a_1a_2 - b_1b_2 + (a_1b_2 + a_2b_1)i$; $0 = 0 + 0\cdot i$;

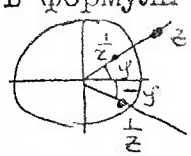
Задача $\mathbb{C} \cong \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,b \in \mathbb{R}\right\}$. Найти характеристику $\mathbb{C}$.

В $\mathbb{C}$ определена инволюция $\mathbb{C} \to \mathbb{C}$: $z = x + iy \mapsto \bar{z} = x - iy$, которая наз. сопряжением. Упражнение I. $z \mapsto \bar{z}$ автоморфизм $\mathbb{C}$.

Упражнение 2. $z\bar{z} \in \mathbb{R}$, $z + \bar{z} \in \mathbb{R}$. $z^{-1} = 1/z = \bar{z}/(z\bar{z}) = x/(x^2+y^2) - iy/(x^2+y^2)$. Аргументом $z = x + iy$ называется угол $\varphi = \mathrm{arctg}\, y/x = \mathrm{arg}\, z$. Модулем $z = x + iy$ называется число $|z| = \sqrt{z\bar{z}} = \sqrt{x^2+y^2}$. В $\mathbb{C}$ нет "естественного" порядка. Введем на плоскости $\mathbb{C}$ полярные координаты. $x = r\cos\varphi$; $y = r\sin\varphi$; $z = r\cos\varphi + ir\sin\varphi = r(\cos\varphi + i\sin\varphi)$, $|z| = r$, $\mathrm{arg}\, z = \varphi$. $z' = r'(\cos\varphi' + i\sin\varphi')$. Тогда $zz' =$ (выкладки выполнить самим) $= rr'(\cos(\varphi+\varphi') + i\sin(\varphi+\varphi'))$

Это можно сформулировать в виде:

Лемма. При перемножении комплексных числе модули их перемножаются, а аргументы складываются. /Отсюда простой способ запомнить формулы тригонометрии/. Следствие: $z^{-1} = \frac{1}{r}(\cos\varphi - i\sin\varphi)$



Мультипликативный характер $e: \mathbb{R} \to \mathbb{R}$ / $e^{\varphi_1+\varphi_2} = e^{\varphi_1}\cdot e^{\varphi_2}$

Формула Эйлера: $\cos\varphi + i\sin\varphi = e^{i\varphi}$!

Но e^x – вполне определенная функция. Как ее определить для $\mathbb{C}$? Нужно определение, в котором участвуют только операции поля. $e^x = 1 + x + x^2/2 + \ldots$

$e^{i\varphi} = 1 + i\varphi + \frac{(i\varphi)^2}{2!} + \ldots + \frac{(i\varphi)^n}{n!} + \ldots = 1 - \frac{\varphi^2}{2!} + \frac{\varphi^4}{4!} - \frac{\varphi^6}{6!} + \ldots + i(\varphi - \frac{\varphi^3}{3!} + \frac{\varphi^5}{5!} - \ldots)$. Но $\cos\varphi = 1 - \frac{\varphi^2}{2!} + \frac{\varphi^4}{4!} + \ldots$; $\sin\varphi = \varphi - \frac{\varphi^3}{3!} + \frac{\varphi^5}{5!} + \ldots \Rightarrow e^{i\varphi} = \cos\varphi + i\sin\varphi$! Значит, $z = |z|e^{i\varphi}$ $z' = |z'|e^{i\varphi'}$ и $zz' = |z|\cdot|z'|\cdot e^{i(\varphi+\varphi')}$

Упражнение. Построить $e^{i\frac{\pi}{2}}$, $e^{i\pi}$, $e^{i\pi/6}$, $e^{i\pi/3}$, $e^{i\pi k}$, $e^{-i\frac{\pi}{2}}$.

Корни: $z^n = w$; $z^n = |w|e^{i\arg w}$ $|z|^n = |w|$, $n\arg z = \arg w \Rightarrow \begin{cases} |z| = \sqrt[n]{|w|} \\ \arg z = \frac{\arg w + 2\pi k}{n} \end{cases}$

Упражнение. Построить $\{\sqrt[5]{1}\}$, $\{\sqrt[3]{-1}\}$, $\{\sqrt{i}\}$.

Задача. $\sqrt[n]{1}$ образуют циклическую группу по умножению.

Задача. $K_2 = \{a + bj \mid j^2 = 1\}$ $K_\Pi = \{a + bj \mid j^2 = 0\}$. а) Изоморфны ли K_2 и K_Π ? Пусть $K_{p,q} = \{a + bj \mid j^2 = p + jq\}$ б) Описать, при каких (p,q) $K_{p,q}$ изоморфно C ; K_2; K_Π ? в) Для K_2 построить "тригонометрическую форму" чисел.

Отступление 2. Конечные поля.

F – конечное поле. $Char\, F = p$. Тогда $\mathbb{F}_p \hookrightarrow F$. Это означает, что элементы из F можно складывать между собой и умножать на элементы из $\mathbb{F}_p$; т.е. F – векторное пр-во над $\mathbb{F}_p$! Пусть $\dim_{\mathbb{F}_p} F = n$. Выберем базис $e_1, \ldots, e_n$. Тогда $\forall a \in F$ $a = \sum_{i=1}^{n} \alpha_i e_i$, где $\alpha_i \in \mathbb{F}_p$. $\Rightarrow |F| = p^n$. Поэтому F обозначается $\mathbb{F}_{p^n}$.

Лемма. $\forall a \in \mathbb{F}_{p^n}$ является корнем некоторого многочлена $p(x) \in \mathbb{F}_p[X]$.

Д-во. В $\mathbb{F}_{p^n}$ рассмотрим элементы $1, a, a^2, \ldots, a^n$. Т.к. $\dim_{\mathbb{F}_p} \mathbb{F}_{p^n} = n$, то они линейно зависимы. $\Rightarrow \exists \alpha_n, \alpha_{n-1}, \ldots, \alpha_0$, не все равные 0, такие что $\alpha_n a^n + \alpha_{n-1} a^{n-1} + \ldots + \alpha_0 = 0$. Но это означает, что a является корнем мн-на $p(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_0$ ▷

Определение. Элемент $a \in F_I$ (F_I – расширение поля F) называется алгебраическим над F, если $\exists\, p(x) \in F[X]$ такой, что $p(a) = 0$. Если все $a \in F_I$ алгебраичны над F, то F_I наз. алгебраическим расширением F.

Пусть $F_I \supset F$ – расширение поля F. Говорят, что F_I является конечным расширением F, если $\dim_F F_I < \infty$.

$\dim_F F_1 = [F_I : F]$ – наз. степенью расширения. /Замечание $[F_I : F]$ как полей $\neq [F_I : F]$ как аддитивных групп: $[\mathbb{F}_{p^n} : \mathbb{F}_p] = \dim_{\mathbb{F}_p} \mathbb{F}_{p^n} = n$, а $[\mathbb{F}_{p^n} : F]$ как аддитивных групп – p^{n-1}. Не путать!./

Следствие 1. $\mathbb{F}_{p^n}$ является алгебраическим расширением $\mathbb{F}_p$.

Следствие 2. Если $[F_I : F] < \infty$, то F_I – алгебраическое расширение F.

Рассмотрим, например, $\Gamma_8 = \Gamma_{23}$. В $\mathbb{F}_2[X]$ рассмотрим $p(x) = 1 + x + x^3$; $p(x)$ неприводим (нет корней). Введем $\Gamma_8 = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{F}_2,\ \alpha^3 = \alpha + 1\}$ $\pi : \mathbb{F}_2[X] \xrightarrow{\text{эпи}} \mathbb{F}_8$. $\pi(f(x)) = f(\alpha)$. $\ker \pi = \{g(x) \mid g(\alpha) = 0\} = (p(x)) \Rightarrow \mathbb{F}_8 \cong \mathbb{F}_2[X]/(p(x))$

Задача $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^k} \iff n \mid k$.

— x —

Теорема: $\forall F\ \exists F_I$: всякий многочлен $f(x) \in F[X]$ имеет в F_I корень.

Д-во будет использовано (и напомнено) ниже.

Лекция 12. §5. Алгебраические расширения

Определение. Пусть p: $F[X] \to E$ (где E – расширение поля F), такой, что $p|_F = id_F$ и p: $X \mapsto \alpha$ имеет ненулевое ядро. $\ker p = (p(x))$ /напомним, что (t) – обозначает главный идеал , порожденный элементом t/. $P(x)$ неприводим. Можно считать, что $a_n = 1$. Такой $p(x) = Irr(\alpha, F, X)$, однозначно определенный элементом α , наз. неприводимым многочленом α над F.

Предложение 1. $[E:F]=n<\infty \Rightarrow E$ алгебраично над F. Обратное предложение неверно: а) $E\subset\mathbb{C}$: $E=\{\alpha\in\mathbb{C} \mid \alpha$ алг. над $\mathbb{Q}\}$ $E\supset\mathbb{Q}$ – алгебраическое, но $[E:\mathbb{Q}]=\infty$ б) к – поле; $E=\bigcup_{k\in I}E_k$, где $[E_k:k]<\infty$ $E\supset k$ – алг., но $[E:k]=\infty$.

Предложение 2. $k\subset F\subset E$ – расширения. Тогда: а) $[E:k]=[E:F]\cdot[F:k]$ и б) если $\{f_i\}_{i\in I}$ – базис F над к и $\{g_j\}_{j\in J}$ – базис E над F, то $\{f_i g_j\}_{(i,j)\in(I,J)}$ базис E над к. Док-во. $\{f_i g_j\}$ – порождающая система (все суммы конечные); легко видеть, что они линейно независимы. Все.

Пусть $E\supset F\supset k$. $[E:k]<\infty \Leftrightarrow [E:F]<\infty$ и $[F:k]<\infty$

Определение. $k\subset E$. $\alpha\in E$. $k(\alpha)$ обозначает наименьшее подполе E, содержащее к и α. Проверьте, что $k(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)} \mid f,g\in k[x],\ g\neq 0\right\}$.

Предложение 3. $E\supset k$ $E\ni\alpha$ алгебраично над к. Тогда $k(\alpha)=k[\alpha]$./Напомним, что $k[\alpha]=\{f(\alpha)\mid f(x)\in k[x]\}$, $[k(\alpha):k]=n<\infty$ и $n=\deg \operatorname{Irr}(\alpha,k,x)$

Док-во. вспомним первое определение лекции 12: $p: k[X]\to E$ $k[\alpha]=\operatorname{Im}p=k[X]/(p(x))$ – поле $\Rightarrow k[\alpha]\supset k(\alpha)$, но $k[\alpha]\subset k(\alpha)\Rightarrow k[\alpha]=k(\alpha)$. $1,\alpha,\ldots,\alpha^{n-1}$ – линейно независимы над к (т.к. $p(x)=\operatorname{Irr}(\alpha,k,X)$ – наименьшей степени). Для всякого $f(x)\in k[X]$ $f(x)=q(x)p(x)+r(x)$ причем $\deg r(x)<\deg p(x)\Rightarrow f(\alpha)=r(\alpha)\Rightarrow 1,\alpha,\ldots,\alpha^{n-1}$ порождают $k[\alpha]$. Все.

Следствие. "Трисекция угла" и "удвоение куба" – классические задачи древности о построении с помощью циркуля и линейки – неразрешимы.

Трисекция угла. Задача ставится так: указать алгоритм, последовательность построений, с помощью которых по любому данному углу φ строится угол $\varphi/3$. Т.к. дана еще единица масштаба (или ее можно выбрать произвольно), то можно считать, что задано комплексное число $z=e^{i\varphi}$. Трисекция сводится к построению $w=e^{i\varphi/3}$. w удовлетворяет уравнению $w^3=z$. Пусть $k=\mathbb{Q}(z)$; $x^3-z=\operatorname{Irr}(w,k,X)$; $\mathbb{Q}(w)=E$; $[E:k]=3$ (см. предложение 3). С помощью циркуля и линейки мы можем расширять наше первоначальное поле $k\subset E_1\subset E_2\subset\ldots$, но только так, чтобы $[E_k:E_{k-1}]=2$! Но $3\neq 2^m$ (см. предложение 2).

Удвоение куба. Идея та же. В этой задаче надо строить $w=\sqrt[3]{2}$. Дать подробное доказательство самостоятельно.

$E\supset k\subset F$, $E\subset L$ и $F\subset L$. EF обозначает наименьшее подполе L, содержащее E и F. EF называется композитом полей E и F. Вместо $E\supset k$ рисуют такую диаграмму: $\begin{matrix}E\\k\end{matrix}$ верхнее поле содержит нижнее.

$k\subset E\ni\alpha_1,\ldots,\alpha_n$ $k(\alpha_1,\ldots,\alpha_n)=\{$наименьшее подполе E, содержащее к и $\alpha_1,\alpha_2,\ldots,\alpha_n\}$. Ясно, что $k(\alpha_1,\alpha_2,\ldots\alpha_n)=\left\{\frac{f(\alpha_1,\alpha_2,\ldots,\alpha_n)}{g(\alpha_1,\alpha_2,\ldots\alpha_n)} \mid g\neq 0\right\}$.

Определение. E – конечно порождено над к, если $\exists\alpha_1,\alpha_2,\ldots,\alpha_n\in E$, такие, что $E=k(\alpha_1,\alpha_2,\ldots\alpha_n)$.

Предложение 4. $E\supset k$ – конечное расширение $\Rightarrow E$ конечно порождено над к. Д-во. $\alpha_1,\ldots\alpha_n$ – базис E над к $\Rightarrow E=k(\alpha_1,\alpha_2,\ldots\alpha_n)$; все.

Если $E=k(\alpha_1,\ldots\alpha_n)$, $k\subset F\subset L$; $E\subset L$, то $EF=F(\alpha_1,\alpha_2,\ldots\alpha_n)$.

Далее, если $L\supset F\supset k$ и $L\ni\alpha$ – алгебраич. над к $\Rightarrow\alpha$ – алгебр. над F.

Лемма. Пусть $k\subset k(\alpha_1)\subset k(\alpha_1,\alpha_2)\subset\ldots\subset k(\alpha_1,\alpha_2,\ldots,\alpha_n)$, α_i алг. над к. Тогда $k(\alpha_1,\alpha_2,\ldots,\alpha_n)$ конечное алг. расширение над к. /Для док-ва воспользоваться тем, что $k(\alpha_1,\alpha_2)=k(\alpha_1)(\alpha_2)$ и предыдущим замечанием./

Следствие. Конечно порожденное алгебраическое расширение – конечно.

Пусть теперь α не алгебраично над 0. В качестве α можно взять π или e,

если известно, что они трансцендентны. Можно также выбрать $\alpha = 0,110001\ldots$ (1 стоят на местах с номерами, равными $n!$).
Задача. Док-ть, что это число трансцендентно. (Указание. Сначала доказать следующую лемму: если β алгебраично над $\mathbb{Q}$, то $\exists\, n \in \mathbb{N}$ и $C > 0$ такие, что $\forall\, p/q \quad |\beta - p/q| > C/(q)^n$. ($\alpha$ таким свойством не обладает.) $\mathbb{Q}(\alpha)$ конечно порождено над $\mathbb{Q}$, но не конечно.

§ 6 Алгебраическое замыкание.

В этом параграфе будут доказаны два основных утверждения:
Теорема 1. Для $\forall$ к $\exists$ $E \supset$ к такое, что в E любой многочлен $f \in E[X]$ имеет корень.
Теорема 2. Поле E в предыдущей теореме можно выбрать алгебраическим над к.
1. Было доказано утверждение: к – поле $p(x) \in$ к$[X]$ – неприводимый многочлен, тогда $\exists$ $F \supset$ к: $p(x)$ имеет в F корень. Такое расширение поля к называется присоединением корня $p(x)$. Следствие из этого утверждения такое: Пусть F – поле $f_1, f_2, \ldots, f_n \in F[X]$. Тогда $\exists$ $E \supset F$ такое, что $\forall f_i$ имеют в E корень. (Естественно, надо последовательно присоединять корни f_i).

Определение. Поле E наз. алгебраически замкнутым, если всякий $f \in E[X]$ имеет в E корень.
Замечание. Если E алгебраически замкнуто, то всякий многочлен степени n из $E[X]$ имеет в E n корней.
Теорема 1. Для всякого поля к существуют алгебраически замкнутое поле $E \supset$ к.
Док-во. Конструкция Артина. Построим $E_1 \supset$ к такое, чтобы все $f \in$ к$[X]$ имели бы в E_1 корни. Для любого $f \in$ к$[X]$ рассмотрим символ x_f. В кольце к$[\{x_f\}]$ (неизвестными являются все символы $\{x_f\}_{f \in K[x]}$) рассмотрим идеал, порожденный многочленами $\{f(x_f)\}$, $-\mathcal{T}$. Утверждается, что $\mathcal{T} \neq$ к$[\{x_f\}]$. Действительно, если это не так, то $1 = g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \ldots + g_k f_k(x_{f_k})$ (ж), где $g_i \in$ к$[\{x_f\}]$.

Рассмотрим расширение поля к$\subset$F, в котором лежат корни многочленов $f_1, \ldots, f_k$ (следствие 2). к$[\{x_f\}] \subset F[\{x_f\}]$. В кольце $F[\{x_f\}]$ соотношение (ж) тоже должно выполняться. Но в F есть элементы $\alpha_1, \ldots, \alpha_k$ такие, что $f_i(\alpha_i) = 0$. Подставив (ж) вместо x_{f_i} α_i, получим $1 = 0$. Противоречие.

Пусть м – максимальный идеал, содержащий $\mathcal{T}$. $E_1 =$ к$[\{x_f\}]/$м – поле. В E_1 любой многочлен $f(x) \in$ к$[X]$ степени ≥ 1 имеет корень: класс x_f. Можно сказать что E_1 получается присоединением всех корней всех многочленов к$[X]$.

Теперь можно построить $E_2 \supset E_1$, присоединив корни всех многочленов из $E_1[X]$ затем $E_3 \supset E_2$ и т.д. к$\subset E_1 \subset E_2 \subset \ldots$ Рассм. $E = \cup E_i$. E – поле. E алгебраически замкнуто.

Следствие. Для любого к существует алгебраическое над к алгебраически замкнутое поле $\bar{k}$ (оно наз. алгебраическим замыканием поля к).
Док-во. $\bar{k} = \bigcup_{i \in I} F_i$, где F_i – алгебраично над к. Можно считать, что мы сначала построили E – алгебраически замкнутое поле, содержащее к, и в нем рассматриваем объединение всех алгебраических элементов над к. Докажем, что $\bar{k}$ – алгебраически замкнуто. Пусть $\alpha \in E$ и алгебраично над $\bar{k}$. Тогда $\exists$ $a_0, a_1, \ldots, a_n$ из $\bar{k}$ такие, что $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Рассмотрим $k(a_0, \ldots, a_n) \supset$ к – это расширение конечно порожденное. Все a_i – алгебраические над к, следовательно, $k(a_0, \ldots, a_n) \supset$ к – конечное расширение. $k(a_0, \ldots, a_n, \alpha) \supset k(a_0, \ldots, a_n)$ – алгебраическое, следовательно, конечное. Получаем, что $k(a_0, \ldots, a_n, \alpha) \supset$ к – ко-

нечное, следовательно, алгебраическое $\Rightarrow \alpha$-алгебраично над $k \Rightarrow \alpha \in \bar{k}$. $f(x) \in \bar{k}[X]$. f имеет корень α в E. α алгебраичен над $\bar{k}$, и $\alpha \in k$. Следовательно, k – алгебраически замкнуто. *Все.*

Х. Алгебраическое замыкание поля k определено однозначно с точностью до изоморфизма. Это следует из такого утверждения: пусть k – поле и E и E' – алгебраические расширения над k. Если E, E' алгебраически замкнуты, то существует изоморфизм $\tau : E \to E'$ поля E на E', индуцирующий тождественное отображение на k (см. Ленг, "Алгебра", стр. 196–197).

Приложение I. $\bar{\mathbb{Q}} \neq \mathbb{C}$. Как вы знаете из курса анализа, $\mathbb{C}$ – алгебраически замкнуто. $\bar{\mathbb{Q}}$ – подполе $\mathbb{C}$, состоящее из всех чисел, алгебраических над $\mathbb{Q}$ (или просто алгебраических числе). $\mathbb{C}$ несчетно, а $\bar{\mathbb{Q}}$ – счетно. Действительно, алгебраических чисел "не больше", чем всех многочленов с коэффициентами из $\mathbb{Q}$. Последние представляются в виде объединения счетного числа счетных множеств – многочленов с коэффициентами из $\mathbb{Q}$ фиксированной степени. Это дает еще одно доказательство (не конструктивное, правда) сущетсвования трансцендентных числе. Видно, что трансцендентных чисел "существенно" больше, чем алгебраических. Вообще, верна следующая лемма:

Если F – не коненчое поле, а $E \supset F$ – алгебраическое расширение, то мощности F и E равны.

Приложение 2. Существование $\mathbb{F}_{p^n}$. Мы знаем, что если $\mathbb{F}_{p^n}$ существует, то $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Вспомним, что если $k[X] \ni p(x)$ – неприводим, и $\deg p(x) = n$, то $[k[X]/(p(x)) : k] = n$. Естественно, постараться доказать, что в $\mathbb{F}_p[X]$ существуют неприводимые многочлены любой степени n. Будем рассматривать только приведенные многочлены, т.е. те, у которых старший член с коэффициентом I.

Пример. $p=2$, $k = \mathbb{F}_2$.

степени	I	2	3. $G: X^3; (x+1)^3 = x^3 + x^2 + x + 1; x^2(x+1); x(x+1)^2 = x^3 + x; (x^2+x+1)x$
многочлены со ст. коэфф. I			
приводимые	$O: -$	$3: x(x+1) = x^2 + x;$ $x^2; (x+1)^2 = x^2 + 1.$	
неприводимые	$2: X$ и $X+1$	$x^2 + x + 1$	$2: x^3 + x + 1; x^3 + x^2 + 1$

Задача. Заполнить графу $n=4$; в случаях $n=1,2,3,4$ вывести формулы для числа приводимых и неприводимых многочленов в $\mathbb{F}_p[X]$. Вывести формулу для $\psi_n(p)$ – числа неприводимых многочленов степени n в $\mathbb{F}_p[X]$.

Подойдем с другой стороны. Если $\mathbb{F}_{p^n}$ существует, то $|(\mathbb{F}_{p^n})^*| = p^n - 1$, т.е. мультипликативная группа имеет порядок $p^n - 1$. Следовательно, для $\forall \alpha \neq 0, \alpha \in \mathbb{F}_{p^n}$ $\alpha^{p^n - 1} = 1$ или α является корнем многочлена $x^{p^n} - 1$. Добавим еще $\alpha = 0$. $f(x) = x^{p^n} - x$. Все $\alpha \in \mathbb{F}_{p^n}$ являются корнями $f(x)$. Рассмотрим в $\bar{\mathbb{F}}_p$ $\sigma : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$: $\sigma : \alpha \mapsto \alpha^p$. σ – гомоморфизм полей. Действительно, $(xy)^p = x^p y^p$ и $(x+y)^p = x^p + y^p$. (т.к. биномиальные коэфф. сравнимы с 0 по мод. p). Этот гомоморфизм называется гомоморфизмом Фробениуса.

Рассмотрим $\mathbb{F}_n = \{\alpha \in \mathbb{F}_p \mid \sigma^n(\alpha) = \alpha \Leftrightarrow \alpha^{p^n} - \alpha = 0\}$. $\mathbb{F}_n$ – поле (проверьте это!) $\mathbb{F}_n \supset \mathbb{F}_p$. $\bar{\mathbb{F}}_p$ – алгебраически замкнуто, следовательно, $f(x) = x^{p^n} - x = \prod_{\alpha \in F} (x - \alpha)$ (**) в $\bar{\mathbb{F}}_p$. У $f(x)$ нет кратных корней.

Лемма. α является кратным корнем $g(x) \Leftrightarrow \alpha$ – общий корень $g(x)$ и производной $g'(x)$. /Док-во – самим./

$f(x) = x^{p^n} - x$. $f'(x) = p^n x^{p^n - 1} - 1 = -1$. У $f'(x)$ вообще нет корней и, следовательно, у $f(x)$ нет кратных корней. В разложении (**) все α – различные. Из того, что степень $\deg f(x) = p^n$, следует, что $|\mathbb{F}_n| = p^n$, а также, что $[\mathbb{F}_n : \mathbb{F}_p] = n$.

КОНЕЦ I-ого СЕМЕСТРА.

x x x

Лекция I4. Модули.

В этой лекции К – ассоциативное кольцо с единицей.
Левым модулем М над кольцом К (короче, левым К-модулем) наз. абелева группа (М,+) с операцией, обычно записываемой аддитивно, и снабженная операцией умножения слева на элементы кольца К, т.е. отображением К×М → М, /(к,м) ↦ км/ со свойствами: (М1) $к(м_1+м_2) = км_1 + км_2$; (М2) $(к_1+к_2)м = к_1м + к_2м$;
(М3) $(к_1к_2)м = к_1(к_2м)$; (М4) $1м = м$.

Последнее свойство в "старой терминологии" называется унитарностью К-модуля и является лишним, если у К нет единицы.

Упражнение: $0 \cdot м = ?$

Грубо говоря, модуль – это векторное пространство, но не над полем, а над кольцом./Так учил еще А.Б.Сосинский/.

Примеры. а) Любая абелева группа является модулем над кольцом $\mathbb{Z}$. $(n,a) \mapsto na = \underbrace{a + a + \ldots + a}_{n \text{ раз}}$. Проверьте св-ва (М1 – М4).

Упражнение. Любой модуль над $\mathbb{Z}$ является абелевой группой со структурой $\mathbb{Z}$-модуля из примера а).

б) Всякая абелева группа А является модулем над своим кольцом эндоморфизмов $End_{\mathbb{Z}} A$. $End_{\mathbb{Z}} A = \{\varphi : A \to A \mid \varphi$ гомоморфизм$\}$. $(\varphi, a) \mapsto \varphi(a)$. Проверьте М1–М4.

в) К = F – поле. К-модуль М есть просто векторное пространство над F. М = V.

) Пусть К = F[X] – кольцо многочленов над полем F. Что такое К-модуль М? М – абелева группа по сложению. $F \subset F[X]$. М – F-модуль $\Rightarrow$ М = V – векторное пространство. Кроме того, для $\forall v \in V$ должно быть определено $(X, v) \mapsto Xv$, т.е. X можно рассматривать, как отображение $X: V \to V$ со свойствами: $X(v_1+v_2) = Xv_1 + Xv_2$ и $X(av) \overset{М3}{=} (Xa)v \overset{\text{коммут. с F}}{=} (aX)v \overset{М3}{=} a(Xv)$, где $a \in F$.

Эти два свойства означают, что X – линейное отображение (преобразование XX.

Наоборот, если задано линейное преобразование $\alpha : V \to V$, то V можно наделить структурой F[X] модуля, полагая: $f(X)v = f(\alpha)v = a_0v + a_1\alpha(v) + \ldots + a_k\alpha^k(v)$ для всякого $v \in V$ и $f \in F[X]$. Аксиомы М1 – М4 выполнены.

д) Кольцо К является модулем над самим собой /обозначение ${}_К К$/

Аналогичным образом определяется правый К-модуль М: $М \times К \to М$, $(м,к) \mapsto$ $\mapsto мк$. Если К – коммутативно, то понятие правого и левого К-модуля совпадают. Действительно, положив (по определению) мк = км, получим соответствие между правыми и левыми К-модулями. В таких случаях модуль называется просто К-модулем.

Определение. Пусть $М_1$ и $М_2$ – два К-модуля (слово "левый" будем теперь опускать), $\varphi : М_1 \to М_2$ наз. гомоморфизмом К-модулей (или просто К-гомоморфизмом) если $\varphi(м_1 + м_2) = \varphi(м_1) + \varphi(м_2)$; $\varphi(км) = к\varphi(м)$.

Сохраняются и другие понятия теории групп: подмодуль (дать определение всех приводимых ниже аналогов прежних терминов); ядро, образ, изоморфизм модулей, фактор модуль (по подмодулю).

Основная теорема о гомоморфизмах (эпиморфизмах) и две теоремы об изоморфизме дословно переносятся на модули.

Пересечение $\bigcap_i N_i$ любого семейства подмодулей $N_i \subset М$ снова является подмодулем.

На модули легко переносятся также многие понятия из теории векторных пространств. Так, понятия линейной комбинации, линейной зависимости и независимости, системы образующих (модуля или подмодуля), понятие базиса – все это сохраняет свой смысл и в теории модулей.

Упражнение: подсистема линейно независимой системы – линейно независима,

Пример (внимание!) Система из одного элемента может быть линейно зависимой. рассмотрим $\mathbb{Z}_3$ как $\mathbb{Z}$-модуль. Тогда для элемента $м = \bar{2}$ при $6 \in \mathbb{Z}$ система $6м = 6 \cdot \bar{2} = 0$.

Кроме того, не всякая линейно независимая система дополняется до базиса, и вообще, мало модулей имеют базис.

Определение. Модуль называется модулем конечного типа, если у него есть конечная система образующих (не обязательно линейно независимых), и свободным модулем, если у него есть базис (не обязательно конечный).

Замечание. Подмодуль свободного модуля не обязан быть свободным, например, $M = \mathbb{Z}_6 \supset N = 2M = \{\bar{0}, \bar{2}, \bar{4}\}$. M рассматривается как модуль над самим собой.

Определение. M наз. (внутренней) суммой своих подмодулей A и B (запись: $M = A + B$), если $\forall m \in M \ \exists a \in A$ и $b \in B : m = a + b$. Эта сумма наз. прямой, если разложение $m = a + b$ единственно для всякого m. Обозначение: $M = A \dot{+} B$.

Лемма. $M = A \dot{+} B \iff M = A + B$ и $A \cap B = \{0\}$. Док-во провести самим.

Определение. Если A и B – K-модули, то их (внешняя) прямая сумма $A \oplus B$ определяется как множество пар (a,b) с покоординатным сложением и умножением на элементы K.

Лемма. $M = A \dot{+} B$. Тогда $M \cong M_I = A \oplus B$. Док-во провести самим.

Задачи (отступление) Доказать следующие утверждения для групп (не обязательно абелевых): группа G является прямым произведением своих подгрупп G_k, $k = 1, 2, \ldots, n$ (изоморфна "внешнему" прямому произведению $G_1 \times G_2 \times \ldots \times G_n$), если

I1. $\forall g \in G \ g = g_1 \cdot g_2 \cdot \ldots \cdot g_n \ (g_i \in G_i)$; I2. $g_i g_j = g_j g_i \ g_i \in G_i, g_j \in G_j$

I3. Запись I1 – единственна.

2. Док-ть, что условия I1 – I3 выполнены $\iff$ П1 – П3.

П1. $G_k \triangleleft G$ $k = 1, 2, \ldots, n$. П2. $G = G_1 G_2 \ldots G_n$. П3. $\forall k \ G_k \cap \prod_{i \neq k} G_i = E$.

Легко доказать, что прямая сумма свободных модулей свободна. Также легко видеть, что всякий свободный K-модуль конечного типа с базисом $e_1, e_2, \ldots, e_n$ изоморфен $Ke_1 \dot{+} Ke_2 \dot{+} Ke_3 \dot{+} \ldots \dot{+} Ke_n$. и ${}_K K \oplus \ldots \oplus {}_K K$ (n слагаемых).

Теорема: K – целостное кольцо, M – свободный модуль конечного типа над K, $e_1, e_2, \ldots, e_n$ – базис. Тогда всякая система $b_1, \ldots, b_M$ с $m > n$ линейно зависима.

Док-во. $b_1 = \beta_{11} a_1 + \ldots \beta_{1n} a_n$ … $b_M = \beta_{m1} a_1 + \ldots + \beta_{mn} a_n$ | Пусть $\xi_1 b_1 + \ldots + \xi_m b_M = 0$. Это эквивалентно системе: $\begin{cases} \beta_{11}\xi_1 + \ldots + \xi_m \beta_{1n} = 0 \\ \ldots \end{cases}$

$K \hookrightarrow K^*$ – поле. В K^* последняя система имеет ненулевое решение $\xi_1^* \ldots \xi_m^*$. Приведем эти числа к общему знаменателю: $\xi_i^* = \frac{\xi_i}{\gamma} \Rightarrow \xi_1 \ldots \xi_m$ – ненулевое решение в K. Все доказано.

Следствие. Все базисы равномощны. Если мощность базиса конечна, то соответствующее число называется рангом (или размерностью) M.

K-модуль M наз. циклическим, если $M \cong K/(k)$, где (k) – подмодуль ${}_K K$ (или идеал), порождённый элементом k.

Элемент $m \in M$ наз. периодическим, если $\exists k \in K : km = 0$. Модуль, все элементы которого периодические, наз. периодическим модулем.

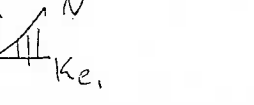
Модуль без периодических элементов наз. модулем без кручения. Совокупность периодических элементов модуля M образует подмодуль, который наз. подмодулем кручения и обозначается $\mathrm{Tor}\, M$.

Пусть K – кольцо главных идеалов и целостное.

Теорема. M – свободный модуль ранга k, $N \subset M$. Тогда N – свободный и $\mathrm{rg}\, N \leq k$.

Док-во. Индукция по k. $k = 1$. $M \cong K$, $N \subset M \iff N$ – идеал в K, но K – кольцо главных идеалов $\Rightarrow N = (a)$, a – базис в N, т.к. K – целостное.

Пусть теперь $\mathrm{rg}\, M = n$, $N \subset M$. $M = M_{n-1} \oplus Ke_1$. Возможны два случая: а) $N \subset M_{n-1}$ тогда все доказано по предположению индукции. б) $\tau = \{k_1 \in K \mid \exists h \in N$ и $h = k_1 e_1 + m', m' \in M_{n-1}\}$ $\tau = (a)$



§ 2. Модули над целостными кольцами главных идеалов

В этой лекции К – целостное кольцо главных идеалов.

Теорема I. Подмодуль А свободного К-модуля М конечного ранга τ свободен, и $\operatorname{rg} A \le \tau$.

Док-во. Индукция по τ.

1. $\tau = I$, $M \cong_K K$, М можно отождествить с К. Тогда А – идеал в К. $A = (a)$ – свободен, и если $A \neq \{0\}$, то $\operatorname{rg} A = I$.

2. Пусть для всех $n < \tau$ теорема верна. $M = M_I \oplus M_{\tau-1}$, где M_I, $M_{\tau-1}$ – свободные подмодули ранга I и $\tau - I$ соответственно.

а) $A \subset M_{\tau-1}$ – тогда по предположению индукции все доказано.

б) $A \not\subset M_{\tau-1}$. Пусть e_I – базис в M_I. Любой элемент $a \in A$ представляется как сумма $a = ke_I + m_{\tau-1}$, где $m_{\tau-1} \in M_{\tau-1}$.

Пусть $S = \{ k \in K \mid \exists\, a \in A \quad a = ke_I + m_{\tau-1} \}$. Тогда $S = \{0\} \iff$ вып. условия п.а). S – идеал (проверьте); $S = (k_I)$ /К – кольцо главных идеалов/ $\Rightarrow$ $\Rightarrow \exists\, \bar{a} \in A \mid \bar{a} = k_I e_I + m_{\tau-1}$. $A_I = A \cap M_{\tau-1}$; A_I – подмодуль $M_{\tau-1}$, $\operatorname{rg} A_I \le \tau - I$. Тогда $A = K\bar{a} \oplus A_I$ (докажите это), и $\operatorname{rg} A \le I + \tau - I = \tau$.

Определение. $m \in M$, где М – К-модуль, наз. периодическим, если $\exists\, k \neq 0$, $k \in K$ такой, что $km = 0$.

Если $\forall\, m \in M$ периодический, то М наз. периодическим модулем. Если в М нет периодических элементов, то М наз. модулем без кручения.

$\operatorname{To}_\tau M = \{ m \in M \mid m$ – периодический$\}$ – образует подмодуль М и наз. подмодулем кручения модуля М.

Теорема 2. М – К-модуль конечного типа без кручения. Тогда М – свободный модуль конечного ранга.

Док-во. Пусть $e_I, \dots, e_n$ – максимально линейно независимая подсистема образующих (она непуста, т.к. e_I – линейно независим, /нет периодических эл-тов/). $A = (e_I, \dots, e_n)$ – свободный подмодуль М. Для любой образующей модуля М, не вошедшей в базис А (обозначим ее b_k), найдутся не равные нулю в совокупности элементы кольца $\bar{k}^{(k)}, \bar{k}_I^{(k)}, \dots, \bar{k}_n^{(k)}$ такие, что $\bar{k}^{(k)} b_k + \bar{k}_I^{(k)} e_I + \dots + \bar{k}_n^{(k)} e_n = 0 \Rightarrow \bar{k}^{(k)} b_k \in A$. b_k-ых – конечное число (т.к. М – модуль конечного типа). Пусть $k = \prod_i \bar{k}^{(i)}$. Рассмотрим морфизм модулей $\sigma : M \to M : \sigma(x) = kx$. Образ $\sigma(M)$ – подмодуль свободного модуля А. По теореме I $\sigma(M)$ – свободный конечного ранга. σ – инъективно (нет ядра). По теореме об эпиморфизме $\sigma(M) \cong M$. Все.

Теорема 3. К- модуль конечного типа М является прямой суммой $M = F \oplus \operatorname{To}_\tau M$, где $F \subset M$ – свободный подмодуль.

Док-во. $f : M \to M/\operatorname{To}_\tau M = M_I$. M_I – без кручения и конечного типа, по теореме 2 M_I – свободный. Пусть $e_I, e_2, \dots, e_n$ – базис M_I. Выберем $a_i \in M$ такие, что $f(a_i) = e_i$. $F = (a_i)$ – подмодуль. /Напомним, что (a_i) обозначает подмодуль порожденный элементами a_i, т.е. $(a_i) = \{ \sum k_i a_i \mid$ сумма конечна $\}$. F – свободный подмодуль (докажите).

а) $M = F + \operatorname{To}_\tau M$. $m \in M$, $f(m) \in M_I \Rightarrow f(m) = \sum k_i e_i$, $\bar{m} = \sum k_i a_i \in F$, $f(m - \bar{m}) = 0 \Rightarrow m - \bar{m} \in \operatorname{Ke}_\tau f = \operatorname{To}_\tau f \Rightarrow m = \bar{m} + (m - \bar{m})$.

б) $M = F \oplus \operatorname{To}_\tau M$, т.к. $F \cap \operatorname{To}_\tau M = \{0\}$. Все доказно.

Определение К-модуль М наз. циклическим (как циклическая группа), если $M \cong K/(k_I)$, $k_I \in K$. Если р – простой элемент в К, то $M(p) = \{ m \in M \mid \exists\, n : p^n m = 0 \}$ является подмодулем М и наз. р-подмодулем. Если $M = M(p)$, то М наз. р-модулем.

Пример. $M = K/(p^{n_1}) + K/(p^{n_2}) + \dots + K/(p^{n_s})$ называется р-модулем типа $(n_I, \dots n_s)$. Договоримся, что $n_1 \le n_2 \le \dots \le n_s$.

Теорема 4. Всякий периодический К-модуль конечного типа М является прямой суммой своих р-подмодулей. /Напомним, что К- целостное кольцо главных идеалов./ $M = \bigoplus_{p \in K} M(p_i)$, p_i - простые, и такое разложение единственно.

Док-во. Для всякого $m \in M$ определим $Ann(m) = \{ k \in K \mid km = 0 \}$. Ann (м) - идеал в К /докажите это/ называется аннулятором элемента м. $Ann(M) = \bigcap_{m \in M} Ann(m)$ - идеал (пересечение идеалов - идеал). $Ann(M) \neq 0$. Действительно, М - конечного типа, $e_1, \ldots, e_n$ - его образующие. Пусть $k_i \in Ann(e_i)$, $k_i \neq 0$ (М -периодический $\Rightarrow$ такие k_i существуют). $\bar{k} = \prod k_i \in Ann(M)$.

К - кольцо главных идеалов $\Rightarrow Ann(M) = (k)$. Это означает, что $\forall m \in M$ $km = 0$. $k = p_1^{n_1} \ldots p_s^{n_s}$ - разложение в произведение простых (оно единственно). Положим $q_i = \prod_{j \neq i} p_j^{n_j}$ (в произведении пропущен i-ый сомножитель). q_i - взаимно просты $\Rightarrow 1 = \sum k_i q_i$. Докажем, что $M = \bigoplus M(p_i)$. Действительно: 1) $\forall m \in M$ $m = 1 \cdot m = (k_1 q_1 + \ldots + k_s q_s) m = k_1(q_1 m) + \ldots + k_s(q_s m)$, $q_i m \in M(p_i)$, т.к. $p_i^{n_i} q_i m = km = 0 \Rightarrow M = \sum M(p_i)$. 2) $\forall p_1, p_2$ $M(p_1) \cap M(p_2) = \{0\}$, т.к. если они пересекаются по м, то $p_1^{s_1} m = 0$, $p_2^{s_2} m = 0$, но $\tilde{k}_1 p_1^{s_1} + \tilde{k}_2 p_2^{s_2} = 1 \Rightarrow m = 1 \cdot m = \tilde{k}_1 p_1^{s_1} m + \tilde{k}_2 p_2^{s_2} m = 0$. Все.

Теорема 5. Любой р-модуль М(р) конечного типа является модулем типа $(n_1, \ldots, n_s)$, т.е. $M(p) = K/(p^{n_1}) + \ldots + K/(p^{n_s})$, и такое разложение единственно.

Док-во. $\forall m \in M(p)$ определим $ord(m) = \{ n \mid Ann(m) = (p^n) \}$ - порядок элемента м. Доказывать теорему будем индукцией по числу образующих.

1° $M(p) = (e)$. Тогда $Ann(e) = (p^n)$ и $M(p) = K/(p^n)$.

2° Пусть для всех $\tau < s$ теорема верна. Выберем среди образующих $e_1, \ldots, e_s$ элемент e_s наибольшего порядка: $ord(e_s) \geq ord(e_i)$ $\forall i$. Ясно, что $ord(e_s) \geq ord(m)$ $\forall m \in M(p)$. $A = (e_s)$ - подмодуль, порожденный элементом e_s, $A \cong K/(p^{ord(e_s)})$. $f: M(p) \to M(p)/A = M_1(p)$. По предположению индукции $M_1(p) = \bar{A}_1 + \ldots + \bar{A}_{s-1}$, $\bar{A}_i = K/(p^{n_i})$, $\bar{A}_i = (\bar{e}_i)$.

Лемма. (о поднятии элемента) $\bar{y} \in M_1(p)$, $ord(\bar{y}) = k$. Существует $y \in M(p)$ такой что $f(y) = \bar{y}$ и $ord(y) = k$.

Док-во. Рассмотрим любой y_1 : $f(y_1) = \bar{y}$. Тогда $p^k y_1 \in \ker f$, следовательно, $p^k y_1 = t_1 e_s$. Пусть $t = p^k t_1$, где р не делится на t_1. Тогда $p^k y_1 = t_1 p^{k_1} e_s$, т.к. $n = ord(e_s) \geq ord(m)$ $\forall m \in M(p) \Rightarrow n \geq k_1$ (если $n = k_1$, то $p^k y_1 = 0$ и все доказано). Умножим $p^k y_1$ на p^{n-k_1}: $p^{n-k_1} p^k y_1 = p^{n-k_1+k} y_1 = t_1 p^n e_s = 0$. Следовательно, $n - k_1 + k \leq ord(y) \leq n = ord(e_s) \Rightarrow k \leq k_1$. Подправим элемент y_1: $y = y_1 - t_1 p^{k_1-k} e_s$. $f(y) = f(y_1) = \bar{y}$ и $p^k y = p^k (y_1 - t_1 p^{k_1-k} e_s) = 0$. $f(p^l m) = p^l f(m) \Rightarrow$ порядок элемента не может уменьшиться. Получаем, что $ord(y) = k$. Лемма доказана.

"Поднимем" элементы $\bar{e}_1, \ldots, \bar{e}_{s-1}$. Получим $\tilde{e}_1, \ldots, \tilde{e}_{s-1}$ такие, что $A_i = (\tilde{e}_i) = K/(p^{n_i})$. Ясно, что $M(p) = A_1 + \ldots + A_{s-1} + A$. Докажем, что эта сумма - прямая. $0 = t_1 \tilde{e}_1 + \ldots + t_s \tilde{e}_s$, $t_i = p^{n_i} \tilde{t}_i$, $\tilde{t}_i \notin (p) \subset K$. $0 = f(0) = f(t_1 \tilde{e}_1 + \ldots + t_{s-1} \tilde{e}_{s-1}) = t_1 \bar{e}_1 + \ldots + t_{s-1} \bar{e}_{s-1} \Rightarrow t_1 = \ldots = t_{s-1} = 0 \Rightarrow t_s = 0$. Следовательно, $M(p) = A_1 \oplus \ldots \oplus A_{s-1} \oplus A$.

Единственность представления: индукция по максимальному порядку. 1° Доказать самостоятельно (или посмотреть конец док-ва).

2° Предположим, что М(р) можно разложить двумя способами, т.е. М(р) представляется двумя типами: $(\underbrace{1, \ldots, 1}_{\mu}, n_1, \ldots, n_l)$ и $(\underbrace{1, \ldots, 1}_{\mu}, m_1, \ldots, m_k)$.

$1 < n_1 \leq n_2 \leq \ldots \leq n_l$ $\quad$ $1 < m_1 \leq m_2 \leq \ldots \leq m_k$

Рассмотрим модуль pM(p), он имеет такие типы: $(n_1-1,\dots,n_\nu-1)$ и $(m_1-1,\dots,m_\mu-1)$, т.к. максимальный порядок у него меньше, то по предположению индукции: $\nu-1=\mu-1$ и $\ell=\kappa$. Осталось доказать, что $\nu=\mu$. Рассмотрим M(p)/pM(p) = = M(p) - модуль, в котором каждый элемент имеет порядок 1. Этот модуль можно рассматривать как модуль над кольцом $K/(p)=K_1$. K_1 - целостное кольцо главных идеалов (при док-ве целостности важно, что (p) - идеал, порожденный простым элементом, такие идеалы называются простыми идеалами).

M(p) - свободный K_1-модуль. Действительно, если $M(p)=A_1\oplus\dots\oplus A_\ell$, где $A_i\cong K/(p^{n_i})$, то $M(p)/pM(p)=A_1\oplus\dots\oplus A_\ell/p(A_1\oplus\dots\oplus A_\ell)=(A_1/pA_1)\oplus\dots\oplus(A_\ell/pA_\ell)$, и $A_i/pA_i\cong K/(p^{n_i})/pK/(p^{n_i})\cong K/pK$, т.е. $M(p)\cong K/(p)\oplus\dots\oplus K/(p)=\underbrace{K_1+\dots+K_1}_{s}$.

У свободного K_1-модуля ранг определен однозначно. Следовательно, $\nu+\ell=\mu+\kappa$, $\ell=\kappa\Rightarrow\nu=\mu$. Это завершает док-во теоремы 5.

Замечание. Теоремы, доказанные нами, можно сформулировать так: пусть M - модуль конечного типа над целостным кольцом главных идеалов K, тогда существуют целое число m, простые элементы кольца K $p_1,p_2,\dots,p_\tau$ и целые числа $n_j^{(i)}$, $i=1,\dots,\tau$; $j=1,\dots,s_i$ такие, что $M\cong\underbrace{K\oplus\dots\oplus K}_{m\text{ раз}}+\underbrace{K/(p_1^{n_1^{(1)}})\oplus\dots\oplus K/(p_1^{n_{s_1}^{(1)}})}_{M(p_1)}+\dots+\underbrace{K/(p_\tau^{n_1^{(\tau)}})+\dots+K/(p_\tau^{n_{s_\tau}^{(\tau)}})}_{M(p_\tau)}$.

Все эти данные можно записать в такую таблицу:

(1)

M							
	p_1	$n_1^{(1)}$	$n_2^{(1)}$	- - - - - -	$n_{s_1}^{(1)}$		
	p_2	$n_1^{(2)}$	$n_2^{(2)}$	- - - - - -			$n_{s_2}^{(2)}$
	⋮	⋮	⋮	⋮	⋮	⋮	⋮
	p_τ	$n_1^{(\tau)}$	$n_2^{(\tau)}$	- - - - - -			$n_{s_\tau}^{(\tau)}$

$n_j^{(i)}\le n_{j+1}^{(i)}$

Следствие: $\operatorname{Ann}(\operatorname{Tor}_\tau M)=(p_1^{n_{s_1}^{(1)}}\cdot\dots\cdot p_\tau^{n_{s_\tau}^{(\tau)}})$

Теорема 6. M- периодический K-модуль, тогда $M=M_1\oplus\dots\oplus M_\Pi$, где каждый M_i - циклический, и $\operatorname{Ann}(M_i)\supset\operatorname{Ann}(M_{i+1})$.

Док-во. Рассмотрим $M_1=K/(p_1^{n_1})+\dots+K/(p_\tau^{n_\tau})$ /все p_i -различные/. Докажем, что $M_1\cong K/(t)$ - циклический, где $t=p_1^{n_1}\cdot\dots\cdot p_\tau^{n_\tau}$. Пусть e_i - образующая модуля $K/(p_i^{n_i})$ /$p_i^{n_i}e_i=0\Leftrightarrow\operatorname{Ann}(e_i)=(p_i^{n_i})$/. Рассмотрим $e=e_1+\dots+e_\tau$. Ясно, что $\operatorname{Ann}(e)=t$, и $(e)\cong K/(t)$. Совпадает ли модуль, порожденный (e) с M_1?

Лемма. (Китайская теорема об остатках). Пусть K - кольцо (Любое, но с единицей), и $\mathcal{T}_1,\dots,\mathcal{T}_n$ - такие идеалы, что $\mathcal{T}_i+\mathcal{T}_j=K$ при всех $i\ne j$. Для любого семейства элементов $x_1,\dots,x_\Pi\in K$ существует $x\in K$ такой, что $x\equiv x_i\pmod{\mathcal{T}_i}$ $\Leftrightarrow x-x_i\in\mathcal{T}_i$ при всех i.

Док-во. Индукция по п. 1° п = 2. $\mathcal{T}_1+\mathcal{T}_2=K\Leftrightarrow\exists k_1\in\mathcal{T}_1$ и $x_2\in\mathcal{T}_2$ такие, что $k_1+k_2=1$. Элемент $x=x_2k_1+x_1k_2$ удовлетворяет условиям леммы (проверьте!)

2° Дальше доказать самим или посмотреть в Ленге стр.82-83 или в Кострикине, стр. 446-447.

Следствие. В условиях китайской теоремы об остатках рассмотрим $f: K\to\prod_{i=1}^{n}K/\mathcal{T}_i$, $f: x\mapsto(x/\mathcal{T}_1, x/\mathcal{T}_2,\dots,x/\mathcal{T}_n)$. Тогда f - эпиморфизм.

Док-во. Это просто переформулировка леммы. Все.

Вернемся к нашему модулю. $M_1=(e_1,\dots,e_\tau)$ порождается $e_1,\dots,e_\tau$, следовательно, $\forall m\in M_1$ $m=x_1e_1+x_2e_2+\dots+x_\tau e_\tau$. Идеалы $(p_1^{n_1}),\dots,(p_\tau^{n_\tau})$ удовлетворяют условию леммы, следовательно, $\exists x\in K$ $x-x_i\in(p_i^{n_i})=\operatorname{Ann}(e_i)$. Тогда

$x(e_I+\ldots+e_\ell) = xe_I+\ldots+xe_\ell = x_Ie_I+\ldots+x_\ell e_\ell = м \Rightarrow M_I$ – циклический.

Если M – периодический K-модуль, то он задаётся таблицей (I) с $м = 0$ (Здесь м – целое число, а не элемент модуля M). $M_П = K/(p_I^{n_1^{(1)}}) \oplus \ldots \oplus K/(p_\ell^{n_{s_\ell}^{(\ell)}})$, показатели степеней – последние в строках таблицы I числа. По доказанному $M_П \cong K/(p_1^{n_1^{(1)}} \cdot \ldots \cdot p_\ell^{n_{s_\ell}^{(\ell)}})$, $M_{П-I} = K/(p_1^{n_1^{(1)}} \cdot \ldots \cdot p_1^{n_{s_1-1}^{(1)}}) \oplus \ldots \oplus K/(p_\ell^{n_{s_\ell}^{(\ell)}})$. Ясно, что $Анн(M_{П-I}) \supset Анн(M_П)$ и т.д.

(показатели степеней – предпоследние в (I) числах).

Следствие. $Анн(M) = (p_I^{n_1^{(1)}} \cdot \ldots \cdot p_\ell^{n_{s_\ell}^{(\ell)}})$.

Задача (к китайской теореме об остатках). Число 12 обладает тем свойством (А) что сумма его собственных делителей $6 + 3 + 4 \geq 12$. Доказать, что $\forall$ п найдется отрезок натурального ряда длины п, для которого каждое из его чисел обладает свойством (А).

§ 3. Применения. Жорданова нормальная форма матрицы линейного преобразования.

I. Конечнопорожденные абелевы группы – $\mathbb{Z}$-модули – рассматривались на семинаре.

2. Жорданова нормальная форма линейного оператора. Пусть V – векторное пространство над K, $\mathcal{A}: V \to V$ – линейный оператор. Пусть K – алгебраически замкнуто, например, $K = \mathbb{C}$. Введем в V структуру K[x] – модуля:

1) V – абелева группа по сложению.
2) умножение на элементы поля – естественное (V – векторное пространство)
3) $\forall v \in V$ положим по определению $x \cdot v \overset{def}{=} \mathcal{A}(v)$.

Проверяется, что все аксиомы модуля выполнены. Обратно, если M – K[x] – модуль, то M – векторное пространство над K, и умножение на x задает в M линейный оператор $\mathcal{A}$: $M \to M$ $\mathcal{A}(м) = x \cdot м$.

Простые элементы в K[x] – это линейные многочлены $(x - \lambda)$ /K – алгебраически замкнуто/. Пусть $V = V_П$ – конечномерное векторное пространство. По структурным теоремам (теорема 3) $V \cong (K[x])^S \oplus Tor V$, но K[x] как векторное пространство бесконечной размерности $\dim_K K[x] = \infty$. Если $\dim_K V_п = п$, то $S = 0$, и V – периодический K[x] – модуль.

Рассмотрим $M \cong K[x]/(x-\lambda)^П$. Напомним, что $f: M_1 \to M_2$ наз. морфизмом K-модулей, если $\forall к \in K$ $f(км_I) = к f(м_I)$, и f – гомоморфизм абелевых групп. Следовательно, если $M \cong K[x]/(x-\lambda)^П$, то у обоих модулей существуют базисы, в которых умножение на x задается одной и той же матрицей.

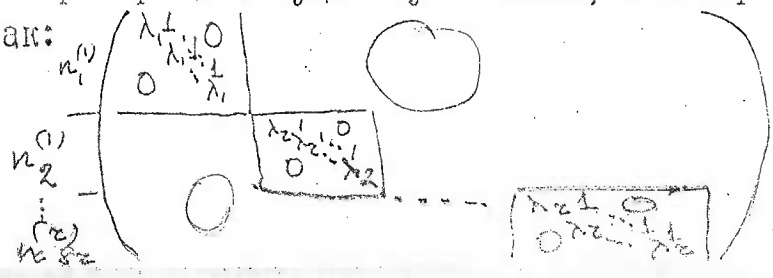
Рассмотрим в $K[x]/(x-\lambda)^П$ базис из элементов $I = e_П$, $(x-\lambda) = e_{П-I}, \ldots, (x-\lambda)^{П-I} = e_I$. Оператор $(x - \lambda)$ действует в этом в этом базисе таким образом: $e_I \to 0$; $e_2 \to e_I; \ldots; e_П \to e_{П-I}$, следовательно, матрица $(x - \lambda)$ в этом базисе

$$\begin{pmatrix} 0 & 1 & & 0 \\ & 0 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$$

Следовательно, матрица оператора $x = (x - \lambda) + \lambda$ в этом базисе

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}$$

Эта матрица наз. жордановой клеткой. Прямой сумме модулей соответствует клеточная структура матрицы линейного оператора $\mathcal{A}$. Существует базис, в котором матрица выглядит так:



Следствие. Для любой матрицы A существует подобная A матрица $B = SAS^{-1}$, такая, что B имеет жорданову форму, S – обратима.

Задачи. I. A – жорданова клетка. Найти минимальный многочлен $P_A(x)$ матрицы A.

2. A – жорданова клетка. Найти $e^A = E + \frac{A}{1!} + \frac{A^2}{2!} + \ldots$

3. V_n – векторное пространство, α – линейный оператор. Рассмотрим V_n как $k[x]$ – модуль. Что такое $V_n(x-\lambda) = M(p)$?

4. $k = \mathbb{R}$, $A^2 = E_n$ – единичная n×n матрица. Доказать, что A подобна $\begin{pmatrix} E_k & 0 \\ 0 & -E_l \end{pmatrix}$ и $k \times l = n$.

5. $k = \mathbb{R}$, $A^2 = -E$. Доказать, что $\dim A = 2n$, и A подобна $\begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix}$

6. $A^2 = A$. Доказать, что A подобна $\begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}$.

7. Привести к жордановой нормальной форме а) $\begin{pmatrix} -1 & 4 \\ -1 & 3 \end{pmatrix}$ в) $\begin{pmatrix} 1 & 15 & -6 \\ 0 & -19 & 8 \\ 0 & -50 & 21 \end{pmatrix}$

8. A приведена к нормальной жордановой форме. Найти минимальный многочлен $P_A(x)$ матрицы A. /Указание: см. Теорему 6 и ее следствия./

9. $P_A(x) \mid \det(A - xE)$ – характеристический многочлен.

10. α – диагонализируемо $\Leftrightarrow$ $P_\alpha(x)$ не имеет кратных корней.

11.* Будем говорить, что клетка $\begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}_k$ соответствует собственному значению λ и имеет размер k. Пусть A – nxn матрица оператора α

а) $n - rg(A - \lambda E)$ = числу клеток, соответствующих собственному значению λ.

б) Обозначим $n_i = rg(A - \lambda E)^i$. Доказать, что $n_{i-1} - n_i$ равно числу клеток, соответствующих λ, размера не меньше i

в) Написать инструкцию, как по числам $n_i(\lambda)$ восстанавливать жорданову нормальную форму A.

Лекция I8. Матрицы над евклидовыми кольцами

E – евклидово кольцо. $A = (\alpha_{ij})$, $\alpha_{ij} \in E$. матрицы

Определение I. Элементарными преобразованиями называются:

I. Перестановки строк и столбцов.

II. Умножение на $e \in E^*$ (делители единицы) всех элементов матрицы.

III. Замена строки (столбца) матрицы суммой её с другой строкой (столбцом), умноженной на любой элемент.

Говорят, что $A \sim B$, если A можно привести к B элементарными преобразованиями

Определение 2. $A \in Mat_n(E)$ наз. унимодулярной, если A обратима.

Лемма I. A унимодулярна $\Leftrightarrow$ $\det A \in E^*$ обратим в E.

Лемма 2. Элементарные преобразования над строками соответствуют умножению на унимодулярную матрицу слева, а над столбцами – справа.

Определение. δ_k = НОД (всех миноров k-го порядка).

Лемма 3. δ_k не меняются при элементарных преобразованиях.

Лемма 4. $\delta_k \mid \delta_{k+1}$.

Лемма 5. $A \sim B$, где $B = \begin{pmatrix} \delta_1 & 0 & \ldots & 0 \\ 0 & \tilde{x}_{22} & \ldots & \tilde{x}_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & \tilde{x}_{n2} & \ldots & \tilde{x}_{nn} \end{pmatrix} = \begin{pmatrix} \delta_1 & 0 & \ldots & 0 \\ 0 & & \tilde{A} & \\ \vdots & & & \end{pmatrix}$

Следствие6. $\delta_1(A) \mid \delta_1(\tilde{A})$.

Определение 3. $A = \begin{pmatrix} e_1 & & 0 \\ & \ddots & \\ 0 & & e_n \end{pmatrix}$, где $e_k \mid e_{k+1}$ называется каноническим видом.

Лемма 7. Любая матрица A может быть приведена к каноническому виду элементарными преобразованиями. /Док-во: индукция по n ⊕ лемма 5. Все./

Следствие 8. $e_к = \frac{\delta_к}{\delta_{к-1}}$ $(\delta_0 = 1)$.

Следствие 9. Для любой матрицы A найдутся унимодулярные матрицы U и P такие, что $UAP = B$ – канонического вида.

Применение. $E = k[\lambda]$ /в этом месте, по традиции, неизвестную обозначают буквой λ /. Мы будем различать матрицы $A(\lambda)$ – матрицы с коэффициентами из E и просто A– матрицы с коэффициентами из k.

По лемме 7 $A(\lambda) \sim \begin{pmatrix} e_1(\lambda) & 0 & \dots & 0 \\ 0 & e_2(\lambda) & & 0 \\ \vdots & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix}$ $e_к(\lambda)$ называются инвариантными множителями матрицы $A(\lambda)$. Их важность определяется следующей теоремой: Теорема 7. A и B подобны $\Leftrightarrow$ $A - \lambda E$ подобна $B - \lambda E$.

Док-во. B подобна $A \Leftrightarrow B = C^{-1}AC$, где $C \in GL(n,k) \Rightarrow C^{-1}(A - \lambda E)C = C^{-1}AC - \lambda C^{-1}EC = B - \lambda E$. Обратно, Пусть $A - \lambda E$ $B - \lambda E$, по лемме это эквивалентно существованию $U(\lambda)$ и $P(\lambda)$ – унимодулярных матриц таких, что $U(\lambda)(A - \lambda E)P(\lambda) = B - \lambda E$. (I) $\Rightarrow$ $\left.\begin{array}{l} U(\lambda)(A-\lambda E) = (B-\lambda E)P^{-1}(\lambda) \\ (A-\lambda E)P(\lambda) = U^{-1}(\lambda)(B-\lambda E) \end{array}\right\}$ (2)

Матрицы $A(\lambda)$, $U(\lambda)$, $P(\lambda)$, $B(\lambda)$ и т.д. можно рассматривать еще и как многочлены от λ с матричными коэффициентами.

Пример. $\begin{pmatrix} \lambda^2 & \lambda^2+3\lambda+1 \\ 2\lambda-1 & \lambda^2+3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\lambda^2 + \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix}\lambda + \begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix}$

Когда можно делить $A(\lambda)$ на $B(\lambda)$? $A(\lambda) = A_n\lambda^n + A_{n-1}\lambda^{n-1} + \dots + A_0$; $B(\lambda) = B_m\lambda^m + B_{m-1}\lambda^{m-1} + \dots$ Можно делить, когда B_m – обратима ($B_m \in GL(n,k)$). Делить можно справа и слева. Рассмотрим $B - \lambda E$. Коэффициент при λ в старшей степени равен $-E$(обратимая матрица) $U(\lambda) = (B-\lambda E)Q_1(\lambda) + R_1$ $\left.\begin{array}{l} \\ P(\lambda) = Q_2(\lambda)(B-\lambda E) + R_2 \end{array}\right\}$ $R_i \in GL(n,k)$ т.к. степень остатка < степени делителя

Рассмотрим (3) $R_1(A-\lambda E)R_2 = (U(\lambda) - (B-\lambda E)Q_1(\lambda))(A-\lambda E)\cdot$
$\cdot(P(\lambda) - Q_2(\lambda)(B-\lambda E)) = U(\lambda)(A-\lambda E)P(\lambda) - U(\lambda)(A-\lambda E)Q_2(\lambda)(B-\lambda E) - (B-\lambda E)\cdot Q_1(\lambda)\cdot$
$\cdot(A-\lambda E)P(\lambda) + (B-\lambda E)Q_1(\lambda)(A-\lambda E)Q_2(\lambda)(B-\lambda E) = (B-\lambda E)\{E - (\dots)(B-\lambda E)\}$

$= (B-\lambda E)P^{-1}(\lambda)$ – здесь воспользовались ур-ниями (2) $\rightarrow (B-\lambda E)P^{-1}(\lambda)$

Выражение в скобках равно 0. Это следует из подсчета коэффициентов степени λ в правой и левой частях (3). Следовательно, $R_1(A-\lambda E)R_2 = B - \lambda E \Rightarrow$ $\left\{\begin{array}{l} R_1R_2 = E \\ R_1AR_2 = B \end{array}\right.$, т.е. A и B подобны! Все.

Задача 1. $A = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{pmatrix}$ – жорданова клетка. Привести $A - \lambda E$ к каноническому виду. Найти $\delta_k(\lambda)$ и $e_k(\lambda)$.

Задача 2. $A = \begin{pmatrix} \lambda_1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_1 \end{pmatrix}$ Задача та же.

–"– 3. $A = \begin{pmatrix} \lambda_1 & 1 & 0 & 0 \\ & \ddots & & \\ 0 & & \lambda_2 & 1 \\ & & & \ddots \end{pmatrix}$ Вопрос тот же.

–"– 4. $A - \lambda E \sim \begin{pmatrix} e_1(\lambda) & & 0 \\ & \ddots & \\ 0 & & e_n(\lambda) \end{pmatrix}$ Тогда $(V, A) \underset{\text{как } k[\lambda]\text{-модули}}{\cong} k[\lambda]/e_1(\lambda) \oplus k[\lambda]/e_2(\lambda) \oplus \dots \oplus k[\lambda]/e_n(\lambda)$,

и это представление есть представление модуля из теоремы 6.

Следствие. Инструкция. I. $A - \lambda E$ привести по $\begin{pmatrix} e_1(\lambda) & & 0 \\ & \ddots & \\ 0 & & e_n(\lambda) \end{pmatrix}$

2. По $e_i(\lambda)$ пишется жорданова нормальная форма B.

3. Если $(A - \lambda E) \sim \begin{pmatrix} e_1(\lambda) & & 0 \\ & \ddots & \\ 0 & & e_n(\lambda) \end{pmatrix} \sim (B - \lambda E)$ посчитать $U(\lambda)$ и $P(\lambda)$ такие, что $U(\lambda)(A-\lambda E)P(\lambda) = B - \lambda E$;

4. $P(\lambda) = Q(\lambda)(B-\lambda E) + R_2$. Тогда $R_2^{-1}AR_2 = B$, т.е. мы нашли не только жорданову нормальную форму, но и матрицу R_2 замены базиса./Курош."Курс..." стр.360-