Лекции 1 – 16 по алгебре и геометрии, 4 семестр

1 Кольца, модули, алгебры, категории

Напомним, что кольцо R – это абелева группа (в аддитивной записи, т.е. с операцией $+$, называемой сложением, и нейтральным элементом 0), в которой имеется вторая операция – умножение (обычно обозначается точкой, или вообще никаким символом не обозначается), причем операции сложения и умножения связаны дистрибутивностью:

$$a(b+c) = ab + ac,$$
$$(b+c)a = ba + ca.$$

Кольцо называется *ассоциативным*, если операция умножения ассоциативна, т.е.

$$a(bc) = (ab)c, \ \forall\, a, b, c \in R.$$

Иными словами, ассоциативное кольцо – это абелева группа относительно сложения и полугруппа относительно умножения и обладающая двусторонней дистрибутивностью относительно сложения и умножения.

Если умножение коммутативно, т.е. $ab = ba, \ \forall\, a, b \in R$, то кольцо называется *коммутативным*.

Если по отношению к умножению имеется в кольце нейтральный элемент, который называют единицей и обозначают как 1, то такое кольцо называют *кольцом с единицей*. В этом случае мы будем считать, что $0 \neq 1$.

Пусть K – кольцо с единицей. Элемент $a \in K$ называется *обратимым*, если существует $b \in K$ такой, что $ab = ba = 1$. В этом случае b называется *обратным* к a и его часто обозначают как a^{-1}. Множество всех обратимых элементов кольца обычно обозначается как K^*. Ясно, что $K^* \subset K \setminus \{0\}$, поскольку 0 – необратимый элемент. Нетрудно видеть, что множество K^*, рассматриваемое с операцией умножения является группой. Единицей этой группы является единица кольца.

Определение 1.1. *Ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим, называется телом.*

Иными словами тело K – это ассоциативное кольцо с единицей такое, что $K^* = K \setminus \{0\}$.

В качестве примера тела можно привести кватернионы $\mathbb{H}$.

Определение 1.2. *Коммутативное тело называется полем.*

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, где p – простое число, – примеры полей.

Понятие подкольца вводится очевидным образом. Это понятие нельзя смешивать с понятием идеала – не всякое подкольцо является идеалом.

Определение 1.3. *Идеал (двухсторонний) I кольца R – это подгруппа в (абелевой группе) R, инвариантная относительно умножения слева и справа на элементы кольца.*

Таким образом, I – идеал, если это подгруппа в R, рассматриваемом только в качестве абелевой группы, и $rI \subset I$ и $Ir \subset I$ для любого $r \in R$. В случае, если выполнено только первое включение, говорят, что I – левый идеал, если – второе, то – правый идеал. Поэтому идеал – это одновременно и левый и правый идеал.

Для идеала используют обозначение аналогичное обозначению нормальной подгруппы, т.е. пишем $I \lhd R$, если I – идеал (двухсторонний), что не удивительно, поскольку идеалы в теории колец играют роль аналогичную роли нормальных подгрупп в теории групп.

Идеал называют собственным, если он не совпадает с нулем (с нулевым идеалом – с идеалом, состоящим из одного нуля), или со всем кольцом. Посление два идеала называют тривиальными.

Гомоморфизм колец – это гомоморфизм подлежащих абелевых групп, согласованный с умножением, т.е. $f : R \to S$ – гомоморфизм колец, если

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b) \ \ \forall\, a, b \in R.$$

Ясно, что образ $\operatorname{Im} f$ является подкольцом в кольце S, в то время как ядро $\operatorname{Ker} f = \{r \in R \mid f(r) = 0\}$ является идеалом в R, поскольку из равенства $f(r) = 0$ следует, что $f(r'r) = f(r')f(r) = f(r') \cdot 0 = 0$ и $f(rr'') = f(r)f(r'') = 0 \cdot f(r'') = 0$ для любых $r', r'' \in R$.

На абелевой факторгруппе R/I по идеалу мы можем ввести операцию умножения

$$\{r + I\} \cdot \{r' + I\} := \{rr' + I\}.$$

Легко проверяется, что так введенное умножение корректно определено и, тем самым на R/I возникает структура кольца. Это кольцо называют *факторкольцом* кольца R по идеалу I. Каноническое отображение $\pi : R \to R/I$, $\pi(r) := \{r + I\}$, как легко проверить, оказывается гомоморфизмом колец. Его так и называют – канонический гомоморфизм. Ясно также, что отображение π сюръективно, и поэтому π – эпиморфизм.

Теорема 1.4 (Теорема о гомоморфизме)**.** *Пусть $f : R \to S$ – гомоморфизм колец. Тогда отображение $r + \operatorname{Ker} f \mapsto f(r)$ корректно определено и является изоморфизмом колец $R/I \cong \operatorname{Im} f$.*

Доказательство. Мы знаем, что указанное отображение является изоморфизмом подлежащих абелевых групп. Остается проверить, что это отображение есть гомоморфизм колец, а это особого труда не составляет. □

Остановимся теперь на прямом произведении и прямой сумме колец. Пусть R, S – два кольца. Их прямое произведение $R \times S$ и прямая сумма $R \oplus S$ – это фактически одно и то же, поскольку как множество и то и другое есть декартово произведение множеств R и S, т.е. множество пар (r, s), $r \in R$, $s \in S$, а операции берутся покомпонентно:

$$(r, s) + (r', s') = (r + r', s + s'), \quad (r, s)(r', s') = (rr', ss'), \ \ r, r' \in R, \ \ s, s' \in S.$$

А налогичным образом определяется прямое произведение и прямая сумма конечного числа колец. Снова между ними разница только в обозначении. Отличия начинаются

когда колец бесконечно много. В этом случае прямая сумма оказывается собственным идеалом в прямом произведении.

Итак, пусть A – множество индексов и для каждого $a \in A$ задано кольцо R_a. Прямое произведение $\prod_{a\in A} R_a$ как множество есть декартово произведение множеств R_a, т.е. его элементами являются наборы $(r_a)_{a\in A}$, $r_a \in R_a$, а сложение и умножение берется покомпонентно:

$$(r_a)_{a\in A} + (r'_a)_{a\in A} = (r_a + r'_a)_{a\in A}, \quad (r_a)_{a\in A}(r'_a)_{a\in A} = (r_a r'_a)_{a\in A}.$$

Прямая сумма $\oplus_{a\in A} R_a$ – это подмножество в прямом произведении, состоящее из наборов, в которых все r_a, кроме конечного числа, равны нулю. Ясно, что с определенными выше операциями на наборах прямая сумма оказывается (двухсторонним) идеалом в прямой сумме. Заметим, что если все кольца – это кольца с единицей, то прямое произведение тоже будет кольцом с единицей, а прямая сумма в случае бесконечного числа индексов единицы иметь не будет.

Определение 1.5. *Алгеброй над полем $\mathbb{K}$ называется векторное пространство A над $\mathbb{K}$, на котором определена операция умножения $A \times A \to A$, ставящая в соответствие паре элементов $a, b \in A$ их произведение $ab \in A$, и удовлетворяющая условиям:*

1. A является кольцом (выполняется свойство дистрибутивности)

2. $(\lambda a)b = a(\lambda b) = \lambda(ab)$ для любых $\lambda \in \mathbb{K}$, $a, b \in A$.

Если A – кольцо с единицей (которую обозначим просто как 1), то свойство 2 означает, что подкольцо элементов вида $\lambda \cdot 1$, где $\lambda \in \mathbb{K}$ лежит в центре $Z(A)$ алгебры A. Такая алгебра называется алгеброй с единицей. Если умножение коммутативно, то алгебру называем коммутативной, если ассоциативно – ассоциативной.

Примеры 1.6. 1. Алгебра многочленов от одной или нескольких переменных (коммутирующих, или нет). Алгебра формальных степенных рядов от одной или нескольких переменных.

2. Алгебра операторов на векторном пространстве. Алгебра квадратных матриц с операциями сложения и умножения.

3. Групповая алгебра: $\mathbb{K}[G] = \{\sum_{g\in G} k_g g \mid k_g \in \mathbb{K},\ g \in G\}$, где G – группа.

Гомоморфизм алгебр, изоморфизм и т.д. определяются очевидным образом. Размерность $\dim_{\mathbb{K}} A$ алгебры A – это размерность векторного пространства A над полем $\mathbb{K}$. Например, на кватернионы можно смотреть как на ассоциативную 4-х мерную алгебру над $\mathbb{R}$, или как на 2-мерную алгебру над $\mathbb{C}$.

Более общее понятие – алгебра над кольцом, где обычно кольцо – это подкольцо в алгебре, лежащее в ее центре и играющее роль поля в определении алгебры над полем.

Модуль над кольцом – одно из основных понятий в общей алгебре, обобщающее как понятие векторного пространства так и абелевой группы.

Пусть R – кольцо (как правило R – коммутативное кольцо с единицей $1 \in R$).

Определение 1.7. *Левым R-модулем называется абелева группа M с операцией умножения на элементы кольца $R\times M \to M,\ (r,m)\mapsto rm$, которая удовлетворяет следующим условиям:*

1) $(r_1r_2)m = r_1(r_2m),\ \forall m\in M,\ \forall r_1,r_2\in R,$

2) $r(m_1+m_2) = rm_1+rm_2,\ \ \forall m_1,m_2\in M,\ \forall r\in R,$

3) $(r_1+r_2)m = r_1m+r_2m,\ \forall m\in M,\ \forall r_1,r_2\in R,$

4) $1\cdot m = m,\ \ \forall m\in M$ *для кольца с единицей.*

Правые модули определются аналогичным образом, но при умножении на элементы кольца последние записывают справа. В частности, условие 1) выглядит так:

$m(r_1r_2) = (mr_1)r_2,\ \forall m\in M,\ \forall r_1,r_2\in R.$

В случае коммутативного кольца структура левого модуля очевидным образом определяет структуру правого модуля поэтому левые (правые) модули называют просто модулями.

Примеры 1.8. 1. Любое кольцо можно рассматривать как модуль над собой (в некоммутативном случае получаются левый и правый модули).

2. Левый (правый) идеал кольца является левым (правым) модулем. Двусторонний идеал является и левым и правым модулем.

3. Векторное пространство – это модуль над полем.

4. Абелева группа – модуль над кольцом целых чисел $\mathbb{Z}$.

Определение 1.9. *Пусть M и N – (левые) R-модули. Отображение $f: M\to N$ называется гомоморфизмом модулей, если f – гомоморфизм абелевых групп, согласованный с умножением элементов модулей на элементы кольца R, т.е. выполнены условия:*

1. $f(m+m') = f(m)+f(m'),\ \forall\, m,m'\in M.$

2. $f(rm) = rf(m),\ \forall\, m\in M,\ \forall\, r\in R.$

Определение 1.10. *Подмодуль $A\subset M$ – это подгруппа в M такая, что $rA\subset A$, $\forall\, r\in R.$*

Ясно, что $\{0\}$ и M – подмодули модуля M. Подмодуль отличный от последних двух называют *собственным.*

Пусть $f: M\to N$ – гомоморфизм (левых) R-модулей. Тогда f – гомоморфизм абелевых групп и ядро $\operatorname{Ker} f = \{m\in M \mid f(m) = 0\}$ и образ $\operatorname{Im} f$ – не только подгруппы, но и подмодули в M и N соответственно. Действительно, мы знаем, что это подгруппы, а из того, что f – гомоморфизм модулей следует, что $f(rm) = rf(m)$ и из этого соотношения сразу видно, что эти подгруппы инвариантны относительно умножения на элементы кольца, т.е. являются подмодулями.

Пусть $A\subset M$ – подмодуль в M. Тогда, как мы знаем, определена факторгруппа M/A. Элементами этой абелевой группы являются классы смежности $\{m+A\}$. Введем модульную структуру положив

$$r\{m+A\} = \{rm+A\},\ r\in R.$$

Отображение $f: M\to M/A$ определенное как $m\mapsto\{m+A\}$ есть модульный гомоморфизм, называемый каноническим гомоморфизмом.

Теорема 1.11 (Теорема о гомоморфизме)**.** *Пусть $f : M \to N$ – гомоморфизм (левых) R-модулей. Тогда отображение $m + \operatorname{Ker} f \mapsto f(m)$ есть изоморфизм, (левых) R-модулей $M/\operatorname{Ker} f \cong \operatorname{Im} f$.*

Так же как для групп вводятся понятия мономорфизма, и эпиморфизма. Гомоморфизм модулей является изоморфизмом тогда и только тогда, когда он одновременно мономорфизм и эпиморфизм. Прямое произведение и прямая сумма R-модулей определяется аналогичным образом как для случая абелевых групп и для колец.

Кольцо есть левый R-модуль над собой. Определим *свободный модуль* как модуль изоморфный прямой сумме R-модулей R над собой. Пусть кольцо содержит единицу. Отобразив единицу в произвольный элемент $m \in M$ некоторого R-модуля M мы сможем очевидным образом продолжить отображение до модульного гомоморфизма $f : R \to M$, определив отображение следующим образом:

$$f(r) = f(r \cdot 1) = rf(1) = rm.$$

Возьмем в M произвольные элементы $m_a \in M$, $a \in X$, где X – некоторое множество индексов. Используя эти элементы мы построим модульный гомоморфизм $\oplus_{a \in X} R_a \to M$, где $R_a = R$. Обозначим единицу кольца $R_a = R$ как $1_a \in R_a$ и отправим ее в элемент m_a, а затем продолжим до модульного гомоморфизма $R_a \to M$, $r_a \mapsto r_a m_a$. Отображение

$$(r_a)_{a \in A} \mapsto \sum_{a \in A} r_a m_a$$

корректно определено, поскольку сумма на самом деле конечна, и легко проверить, что это – гомоморфизм R-модулей. Взяв все элементы модуля M мы получим эпиморфное отображение некоторого свободного модуля на M. Из теоремы о гомоморфизме получаем, что любой модуль является фактормодулем свободного модуля.

Пусть $S \subset M$ – подмножество R-модуля M. Оно порождает подмодуль $\langle S \rangle = \{\sum_i r_i s_i \in M \mid r_i \in R,\ s_i \in S\}$, состоящий из всех конечных линейных комбинаций элементов множества S.

Если $M = \langle S \rangle$, то говорят, что модуль M порожден множеством S, а элементы из S называют порождающими. В случае, если S конечно, говорят, что $M = \langle S \rangle$ – конечно порожденный модуль. В случае $R = \mathbb{Z}$ мы возвращаемся к определениям введенным ранее для абелевых групп.

1.0.1 Тензорное произведение модулей

Пусть M – правый R-модуль, а N – левый R-модуль. В этой ситуации можно определить их тензорное произведение $M \otimes_R N$ над кольцом R. Это – абелева группа в общем случае. Однако, если кольцо коммутативно, тензорное произведение естественным образом наделяется структурой R-модуля. По определению

$$M \otimes_R N = F(M \times N)/\langle S \rangle,$$

где $F(M \times N)$ – свободная абелева группа, порожденная элементами декартова произведения $M \times N$ множеств, т.е. элементы этой свободной абелевой группы – формальные конечные суммы $\sum_i (m_i, n_i)$, и
$S = \{(m+m', n)-(m, n)-(m', n);\ (m, n+n')-(m, n)-(m, n');\ (mr, n)-(m, rn) \mid m, m' \in M,\ n, n' \in N,\ r \in R\}$.

Образ элемента (m, n) при каноническом отображении на фактор обозначают через $m \otimes n$, поэтому элементы тензорного произведения – это конечные суммы $\sum_i m_i \otimes n_i$, причем из определения следует, что имеют место соотношения:

$$(m + m') \otimes n = m \otimes n + m' \otimes n,$$
$$m \otimes (n + n') = m \otimes n + m \otimes n',$$
$$mr \otimes n = m \otimes rn.$$

Если кольцо R коммутативно, то считаем, что $rm = mr$, $rn = rn$. Поэтому можно, предполагая дистрибутивность, ввести модульную структуру на тензорном произведении положив

$$r(m \otimes n) = rm \otimes n = m \otimes rn.$$

В случае когда $R = \mathbb{K}$ – поле, модули суть векторные пространства, и их тензорное произведение – тоже векторное пространство. Получается определение тензорного произведения двух векторных пространств. Далее можно показать, что векторные пространства $U \otimes (V \otimes W)$ и $(U \otimes V) \otimes W$ изоморфны. Классические тензоры – это элементы векторных пространств вида

$$V \otimes \cdots \otimes V \otimes V^* \otimes \cdots \otimes V^*,$$

где V^* – сопряженное (двойственное) векторное пространство, т.е. пространство линейных функционалов на V.

1.1 Категории

Определение 1.12. *Категория $\mathcal{E}$ состоит из класса объектов $A, B, C, \cdots \in \mathrm{Ob}\,\mathcal{E}$ и множеств $\mathrm{Mor}(A, B)$ для каждой упорядоченной пары объектов. Элементы множества $\mathrm{Mor}(A, B)$ называются морфизмами из A в B. Задан закон композиции морфизмов: для всяких трех объектов A, B, C задано отображение
$\mathrm{Mor}(B, C) \times \mathrm{Mor}(A, B) \to \mathrm{Mor}(A, C)$. Если изображать элементы из $\mathrm{Mor}(A, B)$ стрелками $f : A \to B$, то композицию $f : A \to B$ с $g : B \to C$ обозначаем как $g \circ f : A \to C$. При этом выполнены аксиомы:*

1. Если пары объектов различны, то множества морфизмов не пересекаются.

2. Для каждого объекта A имеется элемент $\mathrm{id}_A \in \mathrm{Mor}(A, A)$ такой, что $f \circ \mathrm{id}_A = f$ и $\mathrm{id}_A \circ g = g$ для любых морфизмов $f : A \to B$, $g : C \to A$.

*3. Закон композиции ассоциативен (в случае, когда имеет смысл):
если $f : A \to B$, $g : B \to C$, $h : C \to D$ – морфизмы, то $(h \circ g) \circ f = h \circ (g \circ f)$.*

Примеры 1.13. 1. Категория множеств.

2. Категория групп и гомоморфизмов.

3. Категория R-модулей и их гомоморфизмов. Категория линейных пространств над фиксированным полем (морфизмы – линейные отображения).

4. Категория G-множеств и эквивариантных отображений.

5. Категория колец и гомоморфизмов.

Определение 1.14. *Пусть $\mathcal{A}$, $\mathcal{B}$ – категории. Ковариантный функтор F из $\mathcal{A}$ в $\mathcal{B}$ – это правило, сопоставляющее каждому объекту $A \in \mathrm{Ob}\,\mathcal{A}$ объект $F(A) \in \mathrm{Ob}\,\mathcal{B}$ и каждому морфизму $f : A \to B$ морфизм $F(f) : F(A) \to F(B)$. При этом выполнены условия:*

1. $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ для любого объекта $A \in \mathrm{Ob}\,\mathcal{A}$.

2. $F(g \circ f) = F(g) \circ F(f)$, где $f : A \to B$, $g : B \to C$ – любые морфизмы категории $\mathcal{A}$.

Контравариантный функтор G из $\mathcal{A}$ в $\mathcal{B}$ обращает стрелки, т.е. каждому морфизму $f : A \to B$ категории $\mathcal{A}$ ставит в соответствие морфизм $G(f) : G(B) \to G(A)$ так, что выполнено условие:

$2'$. $G(g \circ f) = G(f) \circ G(g)$, где $f : A \to B$, $g : B \to C$ – любые морфизмы категории $\mathcal{A}$.

Пример 1.15. Стирающий (забывающий) функтор – это ковариантный функтор перестающий учитывать какие-нибудь алгебраические структуры. Например, кольцо является абелевой группой. Поэтому забыв про умножение, получаем ковариантный функтор из категории колец в категорию абелевых групп.

Пример 1.16. Обозначим через **Ab** категорию абелевых групп. Пусть фиксирована абелева группа B. Положим $F(A) := \mathrm{Hom}\,(A, B)$. Нетрудно видеть, что F – контравариантный функтор из категории абелевых групп в себя. Гомоморфизм $F(f) : \mathrm{Hom}\,(A', B) \to \mathrm{Hom}\,(A, B)$ для $f \in \mathrm{Hom}\,(A, A')$ определяется очевидным образом. А именно, пусть $\varphi \in \mathrm{Hom}\,(A', B)$, тогда $F(f)(\varphi) := \varphi \circ f \in \mathrm{Hom}\,(A, B)$.

Введенные понятия оказываются полезными во многих областях математики и, в частности, в дифференциальной геометрии.

2 Поля и формы в $\mathbb{R}^3$

Пусть U – открытое множество в $\mathbb{R}^3$. Обозначим через $\mathrm{Vect}(U)$ векторное пространство гладких векторных полей $\mathbf{A} = P\mathbf{i} + Q\mathbf{j} + R\mathbf{k}$, где P, R, Q – гладкие функции на U, т.е. $P, R, Q \in C^\infty(U)$. Ясно, что $\mathrm{Vect}(U)$ – модуль над кольцом гладких функций $C^\infty(U)$. Очевидно, что это – свободный модуль ранга 3 над $C^\infty(U)$.

Положим $\omega^1_{\mathbf{A}} = Pdx + Qdy + Rdz$ и $\omega^2_{\mathbf{A}} = Pdy \wedge dz + Qdz \wedge dx + Rdx \wedge dy$. Эти формулы определяют взаимно однозначные соответствия между пространствами полей и форм $\mathrm{Vect}(U) \leftrightarrow \Lambda^k(U), \quad k = 1, 2$. Соотношение $\omega^k_{f\mathbf{A}+g\mathbf{B}} = f\omega^k_{\mathbf{A}} + g\omega^k_{\mathbf{B}}$, $f, g \in C^\infty(U)$, $k = 1, 2$, показывает, что пространство гладких полей и пространства гладких 1- и 2-форм изоморфны как модули над кольцом гладких функций.

Формы можно складывать и умножать на функции очевидным образом. Их можно перемножать ($\wedge$ – символ умножения), при этом произведение форм – это форма, размерность которой равна сумме размерностей сомножителей. Правила умножения обычные, но умножение дифференциалов антикоммутативно, т.е., например, $dx\wedge dy = -dy\wedge dx$. Из антикоммутативности умножения дифференциалов следует, например, что $dy\wedge dy = 0$ (аналогично для квадратов остальных дифференциалов). Вычислением проверяется, что

$$\omega^1_{\mathbf{A}} \wedge \omega^1_{\mathbf{B}} = \omega^2_{\mathbf{A}\times\mathbf{B}}, \quad \omega^1_{\mathbf{A}} \wedge \omega^2_{\mathbf{B}} = (\mathbf{A},\mathbf{B})\, dx\wedge dy\wedge dz,$$

где $\mathbf{A}\times\mathbf{B}$ – векторное произведение, $(\mathbf{A},\mathbf{B})$ – скалярное произведение.

Определим теперь операцию взятия дифференциала формы. Для 0-форм, т.е. для гладких функций на U – это взятие дифференциала:

$$f \mapsto df = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy + \frac{\partial f}{\partial z}dz \in \Lambda^1(U).$$

Для 1- и 2-форм полагаем:

$$d\omega^1_{\mathbf{A}} = dP\wedge dx + dQ\wedge dy + dR\wedge dz, \quad d\omega^2_{\mathbf{A}} = dP\wedge dy\wedge dz + dQ\wedge dz\wedge dx + dR\wedge dx\wedge dy.$$

Вычислением проверяется, что

$$df = \omega^1_{\mathrm{grad} f},\ d\omega^1_{\mathbf{A}} = \omega^2_{\mathrm{rot}\mathbf{A}},\ d\omega^2_{\mathbf{A}} = \mathrm{div}\mathbf{A}\, dx\wedge dy\wedge dz.$$

Последовательное взятие двух дифференциалов дает нулевую форму: $d(d\omega) = 0$. Таким образом, $d\circ d = 0$. Это соотношение записывают как $d^2 = 0$. Равенство $d^2 = 0$ дает

$$\mathrm{rot}\,\mathrm{grad} f = 0, \quad \mathrm{div}\,\mathrm{rot}\mathbf{A} = 0.$$

Мы определили формы как некие выражения специального вида, с которыми можно совершать разные действия – перемножать, брать дифференциал и т.п. Как математический объект формы представляют собой алгебру над кольцом гладких функций, но эта алгебра привязана самим своим определением к декартовой системе координат $Oxyz$ в $\mathbb{R}^3$. В других (криволинейных) координатах мы будем иметь изоморфную алгебру, элементы которой записаны через дифференциалы новых переменных. Для того, чтобы найти вид дифференциальной формы в новых координатах нужно выразить функции и дифференциалы с помощью новых переменных.

Замена переменных $f : V \to U$, $x = x(u,v,w)$, $y = y(u,v,w)$, $z = z(u,v,w)$ индуцирует отображение форм $f^* : \Lambda^*(U) \to \Lambda^*(V)$, при котором $f^*(g) = g\circ f \in \Lambda^0(V) = C^\infty(V)$, $g \in \Lambda^0(U) = C^\infty(U)$ и $f^*(dx) = \frac{\partial x}{\partial u}du + \frac{\partial x}{\partial v}dy + \frac{\partial x}{\partial w}dw$, $f^*(dy) = \frac{\partial y}{\partial u}du + \frac{\partial y}{\partial v}dy + \frac{\partial y}{\partial w}dw$, $f^*(dx) = \frac{\partial z}{\partial u}du + \frac{\partial z}{\partial v}dy + \frac{\partial z}{\partial w}dw$.

Например,

$$f^*(dx\wedge dy\wedge dz) = J\, du\wedge dv\wedge dw,$$

$J = \det\begin{pmatrix} \frac{\partial x}{\partial u} & \frac{\partial x}{\partial v} & \frac{\partial x}{\partial w} \\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v} & \frac{\partial y}{\partial w} \\ \frac{\partial z}{\partial u} & \frac{\partial z}{\partial v} & \frac{\partial z}{\partial w} \end{pmatrix}$ – определитель матрицы Якоби отображения f.

3 Дифференциальные формы в $\mathbb{R}^n$

Пусть теперь U – открытое множество в $\mathbb{R}^n$. Тогда $\Lambda^0(U) = C^\infty(U)$ и $\Lambda^i(U) = 0$ при $i > n$, а p-формы при $0 < p \leq n$ – это выражения вида

$$\omega = \sum_{1 \leq i_1 < \cdots < i_p \leq n} f_{i_1 \ldots i_p} dx^{i_1} \wedge \cdots \wedge dx^{i_p} \in \Lambda^p(U), \quad \text{где} \quad f_{i_1 \ldots i_p} \in C^\infty(U).$$

Таким образом, $\Lambda^p(U)$ – свободный $C^\infty(U)$-модуль ранга $C_n^p = \frac{n!}{p!(n-p)!}$.

Умножение $\wedge$ ассоциативно, выполнен закон дистрибутивности, и умножение дифференциалов переменных антикоммутативно: $dx^i \wedge dx^j = -dx^j \wedge dx^i$, для всех $i, j \in \{1, \ldots, n\}$. В частности, $dx^i \wedge dx^i = 0$ для всех $i \in \{1, \ldots, n\}$. Это умножение превращает векторное пространство $\Lambda^*(U) = \Lambda^0(U) \oplus \cdots \oplus \Lambda^n(U)$ в *градуированно коммутативную алгебру над кольцом гладких функций*. Градуированная коммутативность умножения означает, что

$$\omega \wedge \omega' = (-1)^{pq} \omega' \wedge \omega, \quad \omega \in \Lambda^p(U), \quad \omega' \in \Lambda^q(U).$$

Пусть V – открытое множество в $\mathbb{R}^m$ и $f : V \to U$ – гладкое отображение. Тогда f индуцирует отображение форм $f^* : \Lambda^*(U) \to \Lambda^*(V)$, при котором

$$f^*(g) = g \circ f \in \Lambda^0(V) = C^\infty(V), \;\; g \in \Lambda^0(U) = C^\infty(U)$$

и если $f = (f^1, \ldots, f^n)^T : V \to U$ и $(u^1, \ldots, u^m)$ – координаты в $\mathbb{R}^m$, то

$$f^*(dx^i) = d(x^i \circ f) = \sum_{k=1}^m \frac{\partial f^i}{\partial u^k} du^k.$$

Индуцированное отображение f^* линейно и согласовано с умножением форм

$$f^*(\omega \wedge \omega') = f^*(\omega) \wedge f^*(\omega'),$$

т.е. является гомоморфизмом алгебр.

Алгебра $\Lambda^*(U)$ является *дифференциальной* алгеброй: взятие дифференциала функции $f \mapsto df$, $f \in \Lambda^0(U) = C^\infty(U)$, т.е. отображение $d : \Lambda^0(U) \to \Lambda^1(U)$, продолжается до оператора

$$d : \Lambda^*(U) \to \Lambda^{*+1}(U),$$

повышающего размерность на единицу и удовлетворяющего аналогу правила Лейбница

$$d(\omega \wedge \omega') = (d\omega) \wedge \omega' + (-1)^p \omega \wedge d\omega', \qquad \omega \in \Lambda^p(U).$$

Вычисление показывает, что

$$d^{\,2} = 0,$$

т.е. $d \circ d = 0$ и

$$f^*(d\omega) = df^*(\omega).$$

В доказательстве равенства $d^2 = 0$ используется антикоммутативность умножения дифференциалов и равенство смешанных производных у гладких функций.

Пусть $f : V \to U$ и $g : U \to W$ – гладкие отображения, где W – открытое множество в $\mathbb{R}^k$. Тогда $(g \circ f)^* = f^* \circ g^* : \Lambda^*(W) \to \Lambda^*(V)$ (при доказательстве используется инвариантность первого дифференциала).

Таким образом, Λ^* – контравариантный функтор из категории гладких многообразий в категорию дифференциальных градуированных алгебр.

3.1 Свойства тензорного произведения $\cdot \otimes_R \cdot$ и $\mathrm{Hom}_R(\cdot, \cdot)$

Пусть M – правый R-модуль, а N – левый R-модуль и C – абелева группа. *Билинейным отображением* (или R-билинейным) будем называть такое отображение $\varphi : M \times N \to C$, что для любых $m, m' \in M$, $n, n' \in N$ и любого $r \in R$ выполнено:

$$\begin{aligned} \varphi(m + m', n) &= \varphi(m, n) + \varphi(m', n), \\ \varphi(m, n + n') &= \varphi(m, n) + \varphi(m, n'), \\ \varphi(mr, n) &= \varphi(m, rn). \end{aligned}$$

Например, имеется каноническое билинейное отображение

$$\pi : M \times N \to M \otimes_R N, \quad (m, n) \mapsto m \otimes n.$$

Тензорное произведение обладает следующим свойством *универсальности*:

Если $\varphi : M \times N \to C$ – билинейное отображение в абелеву группу C, то существует единственный гомоморфизм $f : M \otimes_R N \to C$ абелевых групп через который пропускается φ, т.е. $\varphi = f \circ \pi$.

Доказательство. По определению

$$M \otimes_R N = F(M \times N)/\langle S \rangle,$$

где $F(M \times N)$ – свободная абелева группа, порожденная всеми элементами декартова произведения $M \times N$. Существует единственный гомоморфизм $F(M \times N) \to C$, при котором базисный элемент (m, n) переходит в $\varphi(m, n)$. Из определения билинейности отображения видно, что элементы из $\langle S \rangle$ при этом гомоморфизме будут переходить в ноль, тем самым корректно определен гомоморфизм факторгруппы, т.е. тензорного произведения, в абелеву группу C. Это и есть искомый гомоморфизм $f : M \otimes_R N \to C$, и поскольку $\pi(m, n) = m \otimes n$, имеем $f(m \otimes n) = \varphi(m, n)$. □

Далее ограничимся для простоты случаем коммутативного кольца.

Как было отмечено выше, если кольцо R коммутативно, то тензорное произведение естественным образом наделяется структурой R-модуля. В этом случае можно считать модули одновременно и правыми и левыми, положив по определению, что $rm = mr$, $r \in R$, $m \in M$, в случае когда на M имеется структура правого (или левого) модуля. Тогда универсальность тензорного произведения можно понимать

в модульном смысле – при определении билинейного отображения $\varphi : M \times N \to C$ считаем, что C – тоже R-модуль и дополнительно требуем, чтобы

$$\varphi(mr, n) = \varphi(m, rn) = r\varphi(m, n).$$

Универсальность тогда означает, что для любого такого φ найдется единственный гомоморфизм R-модулей $f : M \otimes_R N \to C$ такой, что $\varphi = f \circ \pi$.

Гомоморфизмы R-модулей $f : M \to M'$ и $g : N \to N'$ определяют гомоморфизм $f \otimes g : M \otimes_R M' \to N \otimes_R N'$, $m \otimes m' \mapsto f(m) \otimes g(m')$, т.е.

$$(f \otimes g)(m \otimes m') := f(m) \otimes g(m').$$

В частности, нетрудно видеть, что зафиксировав модуль N и сопоставляя модулю M модуль $M \otimes_R N$, а гомоморфизму $f : M \to M'$ – гомоморфизм $f \otimes \mathrm{id}_N$, мы получаем ковариантный функтор $\cdot \otimes_R N$ из категории R-модулей в себя. Аналогичным образом фиксировав первый аргумент получаем ковариантный функтор $M \otimes_R \cdot$ по второму аргументу.

Замечание 3.1. Если кольцо R некоммутативно, то по первому аргументу получаем ковариантный функтор из категории правых R-модулей в категорию абелевых групп, а рассматривая второй аргумент получаем ковариантный функтор из категории левых R-модулей в ту же категорию абелевых групп.

Имеют место естественные изоморфизмы R-модулей (R коммутативно и удалено из обозначений тензорного произведения):

1. $M \otimes N \cong N \otimes M$,
2. $(M \otimes N) \otimes L \cong M \otimes (N \otimes L)$,
3. $(M \oplus M') \otimes N \cong (M \otimes N) \oplus (M' \otimes N)$,
4. $R \otimes M \cong M$.

Отображения из левой части в правую строятся так:

$$\begin{aligned} m \otimes n &\mapsto n \otimes m, \\ (m \otimes n) \otimes l &\mapsto m \otimes (n \otimes l), \\ (m, m') \otimes n &\mapsto (m \otimes n, m' \otimes n), \\ r \otimes m &\mapsto rm. \end{aligned}$$

Утверждение 3 позволяет не ставить скобки в тензорном произведении нескольких модулей. Отметим также, что изоморфизмы 1 и 2 дают изоморфизм

$$M \otimes (N \oplus N') \cong (M \otimes N) \oplus (M \otimes N'),$$

а 1 и 4 приводят к изоморфизму $M \otimes R \cong M$. Явно отображения из левой части в правую для этих изоморфизмов таковы:

$$m \otimes (n, n') \mapsto (m \otimes n, m \otimes n'), \quad m \otimes r \mapsto mr.$$

Рассмотрим теперь функтор $\mathrm{Hom}_R(\cdot\,,\cdot\,)$. Пусть M и N – левые R-модули. Тогда множество (модульных) гомоморфизмов $\mathrm{Hom}_R(M,N)$ является абелевой группой, в которой сумма гомоморфизмов f, $g : M \to N$ определяется очевидной формулой

$$(f+g)(m) := f(m) + g(m).$$

Нетрудно убедиться в том, что $f+g \in \mathrm{Hom}_R(M,N)$. Нулем группы $\mathrm{Hom}_R(M,N)$ является гомоморфизм, переводящий все M в $0 \in N$, а обратный к f гомоморфизм $-f$ определяется формулой $(-f)(m) := -f(m)$.

Аналогичным образом определяется и группа гомоморфизмов в случае правых модулей. В случае коммутативного кольца группа гомоморфизмов наделяется структурой модуля так: $(rf)(m) := rf(m) = f(rm)$. Ясно, что rf – гомоморфизм абелевых групп. То, что он R-линеен следует из коммутативности кольца R:

$$(rf)(r'm) = rf(r'm) = rr'f(m) = r'rf(m) = r'[(rf)(m)].$$

Если зафиксировать первый аргумент и менять второй, то получится ковариантный функтор $\mathrm{Hom}_R(M,\,\cdot\,)$ из категории левых R-модулей в категорию абелевых групп. Зафиксировав второй модуль, получим контравариантный функтор $\mathrm{Hom}_R(\cdot\,,N)$. В случае коммутативного кольца это – фунторы из категории R-модулей в себя.

Последовательность R-модулей и гомоморфизмов

$$\ldots \xrightarrow{f_{n-1}} L_n \xrightarrow{f_n} L_{n+1} \xrightarrow{f_{n+1}} \ldots$$

называется *точной*, если $\mathrm{Ker}\, f_n = \mathrm{Im}\, f_{n-1}$ для любого n. Так точность последовательности

$$0 \longrightarrow L \xrightarrow{f} M$$

означает просто, что f – мономорфизм, а точность последовательности

$$L \xrightarrow{f} M \longrightarrow 0$$

равносильна эпиморфности гомоморфизма f.

Функтор из категории модулей в категориию абелевых групп (или модулей) называется *точным*, если он переводит любую точную последовательность в точную.

Тензорное произведение и $\mathrm{Hom}_R(\cdot\,,\cdot\,)$ не точны. Для функтора $\mathrm{Hom}_R(\cdot\,,\cdot\,)$ справедливы следующие утверждения:

1. Для любого M и любой точной последовательности вида

$$0 \to N' \to N \to N''$$

точна индуцированная последовательность (Hom_R для краткости пишем без R)

$$0 \to \mathrm{Hom}\,(M,N') \to \mathrm{Hom}\,(M,N) \to \mathrm{Hom}\,(M,N'').$$

2. Для любого N и любой точной последовательности вида

$$M' \to M \to M'' \to 0$$

точна индуцированная последовательность

$$0 \to \mathrm{Hom}\,(M'',N) \to \mathrm{Hom}\,(M,N) \to \mathrm{Hom}\,(M',N).$$

Для тензорного произведения имеем:

Теорема 3.2. *Если $M' \to M \to M'' \to 0$ – точная последовательность правых R-модулей, то для любого левого R-модуля N точна последовательность*

$$M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0,$$

и если $N' \to N \to N'' \to 0$ – точная последовательность левых R-модулей, то для любого правого R-модуля M точна последовательность

$$M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0.$$

Если R коммутативно, то для любых R-модулей M, N, P имеется естественный изоморфизм модулей

$$\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

Определим $\eta : \mathrm{Hom}_R(M \otimes_R N, P) \to \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$ следующей формулой

$$[(\eta(f))(m)](n) = f(m \otimes n), \quad f : M \otimes_R N \to P.$$

Можно проверить, что η – изоморфизм.

4 Область целостности

Определение 4.1. *Ненулевые элементы $r, r' \in R$ называются делителями нуля, если $rr' = 0$.*

Поскольку в поле любой отличный от нуля элемент обратим, в поле нет делителей нуля.

Определение 4.2. *Ассоциативное и коммутативное кольцо с единицей без делителей нуля называется областью целостности или целостным кольцом.*

В целостном кольце из равенства нулю произведения двух элементов кольца следует, что по крайней мере один из сомножителей равен нулю. Поэтому можно сокращать на ненулевой элемент, а именно если $rr' = rr''$, где $r \neq 0$, то $r' = r''$. Действительно, имеем $r(r' - r'') = 0$, но поскольку $r \neq 0$ и в кольце нет делителей нуля, получаем, что $r' - r'' = 0$.

В качестве примера целостного кольца можно привести кольцо целых чисел. Еще один пример – кольцо многочленов $R[x]$ с коэффициентами в целостном кольце, и, в частности, кольцо многочленов над полем.

Теорема 4.3. *Целостное кольцо, содержащее конечное число элементов является полем.*

Доказательство. Пусть $|R| < \infty$ и $0 \neq r \in R$. Требуется доказать, что у r есть обратный. Умножение на элемент r определяет гомоморфизм подлежащей абелевой группы в себя. Если $rr' = rr''$, то $r' = r''$, т.е. построенное отображение – инъекция. В силу конечности числа элементов, получаем, что построенное отображение является биекцией. Поэтому найдется элемент $\tilde{r}$ такой, что $r\tilde{r} = 1$. $\square$

Теорема 4.4. *Ассоциативное и коммутативное кольцо с единицей является полем в том и только том случае когда оно не содержит нетривиальных идеалов.*

Пусть R – ассоциативное и коммутативное кольцо и $r \in R$ – некоторый фиксированный элемент. Тогда Rr – идеал, обозначаемый (r). Идеалы такого вида называются *главными*, а кольца, в которых любой идеал главный – *кольцами главных идеалов*.

В качестве примеров колец главных идеалов можно привести кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов $K[x]$ над полем K. Доказательство основано на том, что в этих кольцах можно делить с остатком и подробно будет рассмотрено ниже. Например, для многочленов это означает, что для любого ненулевого многочлена $p(x)$ и произвольного многочлена $f(x)$ существуют единственные многочлены $q(x)$ и $r(x)$, что

$$f(x) = p(x)q(x) + r(x),$$

и $\deg r(x) < \deg p(x)$, где deg – степень многочлена, обладающая, очевидно, свойствами:

$$\deg f(x) = \deg \alpha f(x), \quad \text{где} \quad 0 \neq \alpha \in K,$$
$$\deg(f(x) + g(x)) \leq \max(\deg f(x), \deg g(x)),$$
$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

Из последнего свойства следует, что в кольце многочленов над полем нет делителей нуля. По той же причине кольцо многочленов над областью целостности является целостным кольцом.

Разделив многочлен $f(x)$ на линйный многочлен $x - a$ получим, что либо $f(x)$ делится на $x - a$ и тогда $f(x) = (x - a)h(x)$, либо $f(x) = (x - a)q(x) + c$, где $0 \neq c \in K$. Подставив $x = a$ в это равенство, получаем $c = f(a)$. Это утверждение известно как *теорема Безу: остаток от деления $f(x)$ на $x - a$ равен $f(a)$.*

Если $f(a) = 0$, то $a \in K$ называется корнем многочлена $f(x)$, и из теоремы Безу следует, что $f(x)$ делится на $x - a$. Частное будет иметь степень на единицу меньше степени многочлена $f(x)$. Поэтому у многочлена степени n число корней (с учетом кратности) не превосходит n.

Теорема 4.5. *Кольцо многочленов над полем является кольцом главных идеалов.*

Доказательство. Пусть I – собственный идеал кольца многочленов $K[x]$, где K – поле. Пусть $f(x)$ – многочлен наименьшей степени, содержащийся в I. Покажем, что $I = (f(x))$. Ясно, что $(f(x)) \subset I$. Докажем обратное включение.

Пусть $g(x)$ – произвольный многочлен из идеала I. Поделим $g(x)$ на $f(x)$ с остатком: $g(x) = f(x)h(x)+r(x)$, $\deg r(x) < \deg f(x)$. Поскольку $g(x)$, $f(x)h(x) \in I$, остаток $r(x)$ также принадлежит I. Но $\deg r(x) < \deg f(x)$, а $f(x)$ был выбран как многочлен наименьшей степени, поэтому $r(x) = 0$, и, следовательно $g(x)$ делится на $f(x)$. Таким образом, любой многочлен из I принадлежит главному идеалу $(f(x))$, т.е. $I \subset (f(x))$. □

Многочлен называется *неприводимым*, если его нельзя представить как произведение двух многочленов положительных степеней.

Предложение 4.6. *Если произведение двух многочленов делится на неприводимый многочлен, то на него делится по крайней мере один из сомножителей.*

Доказательство. Пусть $p(x)$ – неприводимый многочлен делящий произведение $f(x)g(x)$ многочленов положительной степени. Предположив противное, т.е. что ни один из сомножителей этого произведения не делится на $p(x)$, мы покажем, что найдутся многочлены $f_1(x)$, $g_1(x)$, произведение которых также делится на $p(x)$, и $\deg f_1(x)g_1(x) < \deg f(x)g(x)$. Это приводит к противоречию, поскольку уменьшая степень произведения мы в результате сможем получить делящийся на $p(x)$ многочлен степени меньшей чем у $p(x)$, что абсурдно.

Поделив многочлены $f(x)$, $g(x)$ с остатком мы видим, что произведение остатков делится на $p(x)$. Таким образом, можно считать, что степени многочленов $f(x)$ и $g(x)$ строго меньше $\deg p(x)$. Частное от деления произведения $f(x)g(x)$ на $p(x)$ обозначим через $k(x)$, т.е. $f(x)g(x) = p(x)k(x)$. Поделим $p(x)$ на $f(x)$ с остатком:

$$p(x) = f(x)q(x) + f_1(x).$$

Остаток $f_1(x)$ не равен нулю, поскольку $p(x)$ неприводим, и $\deg f_1 < \deg f$. Умножим это равенство на многочлен $g(x)$:

$$g(x)p(x) = f(x)g(x)q(x) + f_1(x)g(x) \;\Rightarrow\; g(x)p(x) = p(x)k(x)q(x) + f_1(x)g(x).$$

Положив $g_1(x) = g(x)$, из последнего равенства получаем:

$$f_1(x)g_1(x) = p(x)(g_1(x) - k(x)q(x)),$$

т.е. $f_1(x)g_1(x)$ делится на $p(x)$ и $\deg f_1(x)g_1(x) < \deg f(x)g(x)$. □

Немного другое доказательство использует напоминаемые ниже факты о НОД (наибольший общий делитель) многочленов. Напомним, что НОД многочленов $f_1(x), \ldots, f_n(x)$, не все из которых равны нулю, есть многочлен, делящий каждый из этих многочленов, и делящийся на любой общий делитель этих многочленов.

Пусть неприводимый многочлен $p(x)$ делит произведение $f(x)g(x)$ (и, следовательно, $f(x)g(x) = k(x)p(x)$), но не делит $f(x)$. Тогда $(f(x), p(x)) = 1$ (НОД многочленов $f(x)$ и $p(x)$ равен 1), откуда следует, что найдутся многочлены $u(x)$ и $v(x)$ такие, что $u(x)f(x) + v(x)p(x) = 1$. Умножая это равенство на $g(x)$ получаем:

$$u(x)f(x)g(x) + v(x)p(x)g(x) = g(x) \;\Rightarrow\; u(x)k(x)p(x) + v(x)p(x)g(x) = g(x) \;\Rightarrow$$
$$\Rightarrow\; g(x) = p(x)[u(x)k(x) + v(x)g(x)],$$

т.е. $g(x)$ делится на $p(x)$.

Для нахождения НОД используется алгоритм Евклида. Пусть $\deg f(x) \geq \deg g(x)$. Используя деление с остатком получим:

$$\begin{aligned}
f(x) &= g(x)h_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x);\\
g(x) &= r_1(x)h_2(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x);\\
r_1(x) &= r_2(x)h_3(x) + r_3(x), \quad \deg r_3(x) < \deg r_2(x);\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{k-2}(x) &= r_{k-1}(x)h_k(x) + r_k(x), \quad \deg r_k(x) < \deg r_{k-1}(x);\\
r_{k-1}(x) &= r_k(x)h_{k+1}(x).
\end{aligned}$$

Многочлен $r_k(x)$ является НОД многочленов $f(x)$ и $g(x)$. Действительно, рассматривая последовательно равенства снизу вверх убеждаемся в том, что $r_k(x)$ делит многочлены $f(x)$ и $g(x)$. С другой стороны, двигаясь сверху вниз, мы видим, что если многочлен $q(x)$ делит $f(x)$ и $g(x)$, то он делит $r_1(x)$, далее из второго равенства получается, что $q(x)$ делит $r_2(x)$, и т.д. Из предпоследнего равенства получается, что $q(x)$ делит $r_k(x)$.

Покажем, что если многочлен $d(x)$ есть НОД многочленов $f(x)$ и $g(x)$, то найдутся многочлены $u(x)$ и $v(x)$ такие, что:

$$u(x)f(x) + v(x)g(x) = d(x).$$

На самом деле, достаточно рассмотреть случай взаимно простых многочленов (в этом случае пишем $(f(x), g(x)) = 1$). Действительно, пусть $f(x) = f_1(x)d(x)$ и $g(x) = g_1(x)d(x)$, где $d(x)$ – наибольший общий делитель многочленов $f(x)$ и $g(x)$. Многочлены $f_1(x)$ и $g_1(x)$ взаимно просты, и если $u(x)$ и $v(x)$ – такие многочлены, что $u(x)f_1(x) + v(x)g_1(x) = 1$, то умножив это равенство на $d(x)$, получим нужное равенство $u(x)f(x) + v(x)g(x) = d(x)$.

Обозначим через I идеал, порожденный многочленами $f(x)$ и $g(x)$. Любой элемент идеала I есть многочлен вида $u(x)f(x) + v(x)g(x)$, поэтому он делится на $d(x)$ – НОД многочленов $f(x)$ и $g(x)$. Следовательно, $I \subset (d(x))$. С другой стороны, поскольку в кольце многочленов над полем любой идеал является главным, существует многочлен $h(x)$ такой, что $I = (h(x))$. Далее, $h(x) \in (d(x))$, поэтому $h(x)$ делится на $d(x)$. Кроме того, $h(x)$ делит многочлены $f(x)$ и $g(x)$, поскольку $f(x)$, $g(x) \in I$. Следовательно, $h(x)$ есть НОД многочленов $f(x)$ и $g(x)$ как и $d(x)$ (тем самым $h(x) = \alpha d(x)$, где $0 \neq \alpha \in K$). Поэтому $I = (h(x)) = (d(x))$. В частности, $d(x) \in I$ и, значит, может быть представлен в виде $u(x)f(x) + v(x)g(x)$.

Приведенное рассуждение нетрудно перенести на случай n многочленов.

Теорема 4.7. *Пусть $d(x)$ – НОД многочленов $f_1(x), \ldots, f_n(x)$, которые не все равны нулю. Тогда $d(x)$ может быть представлен в форме*

$$d(x) = u_1(x)f_1(x) + \cdots + u_n(x)f_n(x),$$

где $u_1(x), \ldots, u_n(x) \in K[x]$, причем нетривиальный многочлен наименьшей степени, представимый в такой форме, есть НОД многочленов $f_1(x), \ldots, f_n(x)$.

Поясним как найти представление $u(x)f(x)+v(x)g(x) = d(x)$ с помощью алгоритма Евклида. Это даст еше одно доказательство существования такого представления. Из первого равенства в последовательности равенств алгоритма Евклида видно, что $u_1(x)f(x) + v_1(x)g(x) = r_1(x)$ (где $u_1(x) = 1$, $v_1(x) = -h_1(x)$). Подставив это выражение во второе равенство и приведя подобные получим, что $u_2(x)f(x) + v_2(x)g(x) = r_2(x)$. Далее, это выражение для $r_2(x)$ подставим в третье равенство, и получим, что $r_3(x)$ является линейной комбинацией многочленов $f(x)$ и $g(x)$ с коэффициентами из кольца $K[x]$. Продолжая действрвать дальше таким образом, из предпоследнего равенства найдем, что $r_k(x) = d(x)$ является линейной комбинацией многочленов $f(x)$ и $g(x)$ с коэффициентами из кольца $K[x]$, что и требовалось доказать.

Если поле K содержится в поле L, то мы говорим, что L – *расширение* поля K. Рассмотрим L как векторное пространство над K. Его размерность $\dim_K L$ называется *степенью расширения* поля L над K.

Теорема 4.8. *Пусть $p(x) \in K[x]$ – неприводимый над полем K многочлен. Тогда $L := K[x]/(p(x))$ – поле и степень расширения этого поля над K равна степени многочлена $p(x)$.*

Доказательство. Возьмем ненулевой элемент кольца L. Его можно считать образом многочлена $f(x)$ при каноническом эпиморфизме факторизации $K[x] \to L$. Поскольку элемент нетривиален, многочлен $f(x)$ не делится на $p(x)$. Покажем, что умножение на $f(x)$ в $K[x]$ индуцирует инъективное линейное отображение $L \to L$. Линейность очевидна, а инъективность следует из того, что если произведение $f(x)h(x)$ делится на $p(x)$, то $h(x)$ делится на $p(x)$, поскольку $p(x)$ неприводим и по предположению $f(x)$ не делится на $p(x)$. В силу конечномерности L над K, что будет объяснено ниже, получаем, что построенное линейное отображение является изоморфизмом. Поэтому найдется многочлен $g(x)$ такой, что образ многочлена $f(x)g(x)$ в L равен единице поля $K \subset L$, а это означает, что класс многочлена $f(x)$ обратим.

Обозначим образ многочлена x в L через α. Заметим, что $p(\alpha) = 0$, откуда следует, что α^n является линейной комбинацией над полем K элементов $1, \alpha, \ldots, \alpha^{n-1}$, где $n = \deg p(x)$. Следовательно, α^m и при любом $m > n$ будет выражаться через элементы α^k с $k \leq n-1$. Таким образом, L как векторное пространство над K порождается элементами $1, \alpha, \ldots, \alpha^{n-1}$. Эти элементы независимы, т.е. образуют базис. Действительно, предположим противное. Тогда имеется нетривиальная линейная комбинация этих элементов равная нулю, а это означает, что многочлен, полученный из этой линейной комбинации заменой α на x, делится на $p(x)$, что невозможно в силу того, что его степень меньше степени многочлена $p(x)$. Следовательно, $\dim_K L = n = \deg p(x)$. □

Еще раз отметим, что в процессе доказательства оказалось, что неприводимый над K многочлен $p(x)$ имеет корень α в L. Если через $K(x)$ обозначать, как обычно делается, поле рациональных функций, т.е. дробей $\frac{f(x)}{g(x)}$, $f, g \in K[x]$, с обычными операциями сложения и умножения, то поле L естественно обозначить как $L = K(\alpha)$.

Рассуждения в доказательстве удобно проиллюстрировать с помощью следующей коммутативной диаграммы, в которой вертикальные стрелки – это канонический гомоморфизм факторизации $\pi : K[x] \to K[x]/(p(x)) = L$, верхняя горизонтальная стрелка изображает гомоморфизм умножения на многочлен $f(x)$, $h(x) \mapsto h(x)f(x)$, нижняя – гомоморфизм умножения на $\pi(f(x)) = f(\pi(x)) = f(\alpha)$, $l \mapsto lf(\alpha)$.

$$\begin{array}{ccc} K[x] & \xrightarrow{\cdot f(x)} & K[x] \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ L & \xrightarrow{\cdot f(\alpha)} & L \end{array}$$

Немного другое по форме доказательство того, что L – поле, можно провести следующим образом. Если $f(x)$ не делится на $p(x)$, то из неприводимости многочлена

$p(x)$ следует, что $(f(x), p(x)) = 1$. Поэтому найдутся многочлены $u(x)$, $v(x)$ такие, что $u(x)f(x)+v(x)p(x) = 1$. Применив к этому равенству канонический гомоморфизм факторизации π, получаем $u(\alpha)f(\alpha) = 1_L$, что означает обратимость элемента $f(\alpha)$ в L. Поскольку любой ненулевой элемент в L есть $f(\alpha)$ для некоторого не делящегося на $p(x)$ многочлена $f(x)$, получаем, что любой ненулевой элемент в L обратим, т.е. L – поле.

Если профакторизовать кольцо многочленов по главному идеалу, порожденному многочленом, представимым как произведение двух многочленов положительной степени, то в факторкольце будут делители нуля, и, значит, оно не является полем. Таким образом, $K[x]/(f(x))$ – *поле тогда и только тогда, когда многочлен* $f(x)$ *неприводим.*

Пример 4.9. Рассмотрим $\pi : \mathbb{R}[x] \to \mathbb{R}[x]/(x^2 + 2px + q) = L$, где $p^2 < q$. Многочлен $x^2 + 2px + q$ неприводим над $\mathbb{R}$, поскольку если бы он был разложим, он бы представлялся как произведение линейных многочленов и, значит, имел бы вещественные корни, а не корни $x_{1,2} = -p \pm i\sqrt{q - p^2}$, которые не лежат в $\mathbb{R}$. Следовательно, L – поле, и его степень расширения равна степени многочлена, т.е. $\dim_{\mathbb{R}} L = 2$.

Определим $\varphi : \mathbb{R}[x] \to \mathbb{C}$ формулой $\varphi(f) := f(-p+i\sqrt{q - p^2}) = f(x_1)$, $f \in R[x]$. Имеем:

$$\varphi(f + g) = (f + g)(x_1) = f(x_1) + g(x_1) = \varphi(f) + \varphi(g),$$
$$\varphi(fg) = (fg)(x_1) = f(x_1)g(x_1) = \varphi(f)\varphi(g),$$
$$\varphi(\alpha f) = (\alpha f)(x_1) = \alpha f(x_1) = \alpha\varphi(f), \ \ \alpha \in \mathbb{R}.$$

Таким образом, φ – гомоморфизм $\mathbb{R}$-алгебр, а поскольку $\varphi(1) = 1$, $\varphi(x) = x_1$, и $\langle 1, x_1\rangle$ – базис $\mathbb{C}$ над полем $\mathbb{R}$, получаем, что φ – эпиморфизм. Следовательно, $\operatorname{Im}\varphi = \mathbb{C} \ \Rightarrow \ \mathbb{C} \cong \mathbb{R}[x]/\operatorname{Ker}\varphi$, где $\operatorname{Ker}\varphi = \{f \in \mathbb{R}[x] \mid f(x_1) = 0\}$. Но многочлен с вещественными коэффициентами, имеющий корень x_1 имеет и сопряженный корень x_2, и, следовательно, делится на $(x - x_1)(x - x_2) = x^2 + 2px + q$ по теореме Безу, т.е. $\operatorname{Ker}\varphi = (x^2 + 2px + q)$ – главный идеал, порожденный многочленом $x^2 + 2px + q$. Таким образом, имеем изоморфизм полей

$$\mathbb{R}[x]/(x^2 + 2px + q) \cong \mathbb{C}.$$

В частности, $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Задачи 4.10. Пусть R – кольцо, X – множество, $R^X = \operatorname{Map}(X, R)$ – множество отображений из X в R (множество функций на X со значениями в R). Сумму и произведение функций из R^X определим поточечно.

1) Показать, что кольцо $R^X = \operatorname{Map}(X, R)$ наследует свойства кольца R, т.е. если R ассоциативно, то и R^X тоже, если в R нет делителей нуля, то и в R^X их нет, и т.д.

2) Показать, что если K – поле, то K^X – алгебра над K. Более общо: если A – алгебра над полем K, то A^X также является алгеброй над K.

Пусть $a \in X$ – фиксированная точка. Определим $\varphi : R^X \to R$ формулой $\varphi(f) = f(a)$.

3) Показать, что φ – гомоморфизм колец, $I = \{f \in R^X \mid f(a) = 0\}$ – идеал в R^X и $R \cong R^X/I$.

4) Пусть $X \subset \mathbb{R}^n$ (или более общо: X – метрическое пространство), $K = \mathbb{R}$, $\mathbb{C}$, и рассматривается алгебра непрерывных вещественно–значных (или комплексно-значных) функций на X. Сформулировать и доказать аналоги приведенных выше утверждений для этого случая.

Пусть A, B – ассоциативные алгебры с единицей 1 над полем K, причем A – подалгебра алгебры B. Наименьшую подалгебру алгебры B, содержащую A и элементы $u_1, \ldots, u_n \in B$ будем обозначать через $A[u_1, \ldots, u_n]$. Ее можно понимать как пересечение всех подалгебр, содержащих A и $u_1, \ldots, u_n \in B$. Она состоит из произвольных линейных комбинаций над A всевозможных произведений элементов u_i.

В частности, рассматривая расширение полей $K \subset L$ получаем для элементов $u_1, \ldots, u_n \in L$ подалгебру $K[u_1, \ldots, u_n]$ в L. Эту подалгебру можно понимать также как образ гомоморфизма кольца многочленов $K[x_1, \ldots, x_n] \to L$, при котором $x_i \mapsto u_i$ (аналогичное утверждение имеет место и в случае алгебр, но многочлены, вообще говоря, надо рассматривать от некоммутирующих переменных). Наименьшее подполе в L, содержащее эту подалгебру (или, что равносильно, содержащую K и все элементы $u_1, \ldots, u_n$) будем обозначать как $K(u_1, \ldots, u_n)$. Такое подполе можно понимать как пересечение всех подполей в L, содержащих K и элементы $u_1, \ldots, u_n \in L$, а также как поле частных целостного кольца $K[u_1, \ldots, u_n]$, конструкцию которого мы опишем ниже.

Присоединив корень $\alpha = \pi(x)$ неприводимого многочлена $p(x)$ в $L = K[x]/(p(x))$, мы, согласно теореме, получили, что $L = K[\alpha] = K(\alpha)$. Такое расширение поля K называется *простым*. Степень этого расширения конечна и равна степени неприводимого многочлена: $\dim_K L = \deg p(x)$.

Пусть $f(x) \in K[x]$ – не обязательно неприводимый многочлен.

Определение 4.11. *Полем разложения многочлена $f \in K[x]$ называется расширение L поля K, в котором f разлагается на линейные множители, и L порождается над K корнями многочлена f.*

Гомоморфизмы расширений поля K, тождественные на K, называются *гомоморфизмами над K*.

Мы покажем, что поле разложения любого многочлена существует и единственно с точность до изоморфизма над K.

Предложение 4.12. *Пусть $L = K[x]/(p(x)) = K[\alpha] = K(\alpha)$ – простое расширение поля K, полученное присоединением корня $\alpha = \pi(x)$ неприводимого многочлена $p(x) \in K[x]$, и задан гомоморфизм $\varphi : K \to F$ поля K в некоторое поле F. Гомоморфизм φ продолжается до гомоморфизма $K(\alpha) \to F$ ровно столькими способами, сколько различных корней имеет в F многочлен $\varphi(p) \in F[x]$, полученный из p применением к его корффициентам гомоморфизма φ.*

Доказательство. Гомоморфизм φ дает очевидный гомоморфизм $K[x] \to F[x]$. Кроме того, имеется гомоморфизм алгебр $F[x] \to F$ над полем F, при котором $f \mapsto f(\varphi(\alpha))$. При композиции этих гомоморфизмов многочлен $p(x)$ переходит в 0 тогда и только тогда, когда образ многочлена $p(x)$ в $F[x]$ имеет корень равный $\varphi(\alpha)$. Поэтому только в этом случае такая композиция индуцирует корректно определенный гомоморфизм $K(\alpha) = K[x]/(p(x)) \to F$, и ясно, что этот гомоморфизм продолжает φ. □

Теорема 4.13. *Поле разложения любого многочлена над полем K существует и единственно с точность до изоморфизма над K.*

Доказательство. Пусть $f(x) \in K[x]$. Разложим его в произведение неприводимых сомножителей. Удалив из произведения линейные множители, возьмем неприводимый сомножитель степени большей 1 и рассмотрим соответствующее ему простое расширение. Обозначим полученное поле через K_1. В этом поле у f появляется еще хотя бы один корень α_1, причем $K_1 = K[\alpha_1] = K(\alpha_1)$. Если f еще не разлагается полностью в произведение линейных многочленов, то снова возьмем какой-нибудь неприводимый над K_1 сомножитель степени большей 1 и возьмем соответствующее ему простое расширение $K_2 = K_1(\alpha_2) = K(\alpha_1, \alpha_2)$, и т.д. В результате за конечное число шагов приходим к требуемому расширению.

Осталось доказать единственность. Пусть L и F – два поля разложения многочлена $f(x) \in K[x]$. Пусть

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m = L$$

– последовательность простых расширений. Будем последовательно строить гомоморфизмы $\varphi_i : K_i \to F$, продолжая $\varphi_{i-1} : K_{i-1} \to F$ на K_i, начав с тождественного отображения $\varphi_0 = \mathrm{id}_K : K_0 = K \to K \subset F$. В силу предыдущего Предложения 4.12 это можно сделать. Действительно, пусть $f = p_i q_i$ над K_i, где p_i – неприводимый над полем K_i делитель многочлена $f = \varphi_i(f) \in K[x] \subset F[x]$. Поскольку $f = \varphi_i(p_i)\varphi_i(q_i)$ разлагается над F на линейные множители, многочлен $\varphi_i(p_i)$ имеет корень в F, поэтому φ_i можно продолжить на K_{i+1}.

В результате получаем гомоморфизм $\varphi_m : L \to F$, который является изоморфизмом. Действительно, по построению из Предложения 4.12 в образе φ_m оказываются все корни многочлена $f(x) \in K[x] \subset F[x]$ в F, а по условию поле F как раз и порождается над K этими корнями. □

4.1 Конечные поля

Пусть $\mathbb{F}$ – конечное поле, т.е. поле содержащее конечное число элементов $q = |\mathbb{F}|$. Тогда его характеристика $\mathrm{char}\,\mathbb{F}$ является простым числом $\mathrm{char}\,\mathbb{F} = p$, что немедленно следует из того, что в поле нет делителей нуля. Поскольку $\mathbb{F}$ содержит простое поле $\mathbb{Z}_p = \mathbb{F}_p$, оно является векторным пространством над $\mathbb{F}_p$ и следовательно, $q = |\mathbb{F}| = p^n$, где $n = \dim_{\mathbb{F}_p} \mathbb{F}$. Такое поле обозначают как $\mathbb{F}_q = \mathbb{F}_{p^n} = GF(q)$ (сокращение от Galois field).

Напомним, что группа $\mathbb{F}_q^*$ (по умножению) ненулевых элементов поля является циклической. Ее порядок равен $q-1$. Ниже мы приведем для полноты изложения одно из доказательств этого факта.

Теорема 4.14. *Если $|\mathbb{F}| = q$, то каждый элемент поля $\mathbb{F}$ является корнем многочлена $x^q - x$.*

Доказательство. Ноль, очевидно, является корнем указанного уравнения. Если же $0 \neq a \in \mathbb{F}$, то порядок такого элемента по теореме Лагранжа делит порядок группы $\mathbb{F}_q^* = q - 1$, и поэтому $a^{q-1} = 1$, откуда получаем, что $a^q - a = 0$. □

Теорема 4.15. *Для любого простого p и натурального n существует единственное с точностью до изоморфизма поле $\mathbb{F}_{p^n}$ из p^n элементов.*

Доказательство. Обозначим через L поле разложения многочлена $f(x) = x^{p^n} - x$ над полем $\mathbb{Z}_p = \mathbb{F}_p$. У данного многочлена нет кратных корней так как его производная равна -1, и, значит, взаимно проста с самим многочленом. Поэтому все корни этого многочлена, лежащие в L, различны. Количество таких корней равно $q = p^n$. Докажем, что множество корней образует поле. Действительно, если $f(a) = f(b) = 0$, то $a^q = a$, $b^q = b$, поэтому $(ab)^q = a^q b^q = ab \Rightarrow f(ab) = 0$. Если, кроме того, $b \neq 0$, получаем, что и $f(a/b) = 0$. Далее, биномиальные коэффициенты тривиальны $C_p^k = 0$ при $k \neq 0, p$. Поэтому $(a \pm b)^p = a^p \pm b^p$, откуда следует, что $(a \pm b)^q = a^q \pm b^q$. Следовательно, если a, b – корни многочлена $f(x) = x^{p^n} - x$, то и $a \pm b$ – тоже его корень.

Поскольку поле разложения многочлена единственно с точностью до изоморфизма, теорема доказана. □

Если K – поле ненулевой характеристики p, то отображение $\alpha \mapsto \alpha^p$, $\alpha \in K$, является *эндоморфизмом* (гомоморфизмом K в себя). Этот эндоморфизм называется *эндоморфизмом Фробениуса*. Он инъективен, т.е. является мономорфизмом, поскольку из равенства $a^p = b^p$ вытекает, что $0 = a^p - b^p = (a - b)^p \Rightarrow a - b = 0 \Rightarrow a = b$. Ясно, что в случае конечного поля эндоморфизм Фробениуса является автоморфизмом.

Задача 4.16. Доказать, что неподвижные точки автоморфизма поля образуют подполе.

Теорема 4.17. *Поле $\mathbb{F}_{p^n}$ содержит $\mathbb{F}_{p^m}$ в качестве подполя тогда и только тогда, когда $m|n$.*

Доказательство. Если поле $L = \mathbb{F}_{p^n}$ содержит подполе $K = \mathbb{F}_{p^m}$, то L является линейным пространством над K, откуда следует, что p^n есть степень числа p^m. Отсюда следует, что $m|n$.

Пусть, $m|n$ и $k = n/m$. Тогда $p^n - 1 = (p^m)^k - 1 = (p^m - 1)s$, откуда

$$x^{p^n} - x = x(x^{p^n - 1} - 1) = x(x^{p^m - 1} - 1)S(x) = (x^{p^m} - x)S(x).$$

Таким образом, многочлен $x^{p^m} - x$ делит многочлен $x^{p^n} - x$. Все элементы поля $\mathbb{F}_{p^n}$, являющиеся корнями многочлена $x^{p^m} - x$ (их ровно p^m), образуют подполе поля $\mathbb{F}_{p^n}$. □

Для полноты напомним доказательство следующего утверждения.

Теорема 4.18. *Мультипликативная группа конечного поля является циклической.*

Доказательство. От противного. Предположим, что $|F| = q = p^n$, но мультипликативная группа не является циклической. F^* – абелева группа. Если она не является циклической, то существует число $k < q-1$ такое, что $a^k = 1$ для любого $a \in F^*$. Это означает, что все элементы поля F являются корнями многочлена $x^{k+1} - x$. Таким образом, у многочлена степени $k+1 < q$ есть q корней, что невозможно. □

Задача 4.19. *Показать, что для любого простого числа p и любого $n \in \mathbb{N}$ существует неприводимый многочлен степени n над $\mathbb{Z}_p$.*

4.2 Алгебраические расширения

Определение 4.20. *Пусть L – расширение поля K. Элемент $a \in L$ называется алгебраическим над K, если он удовлетворяет какому-либо нетривиальному алгебраическому уравнению с коэффициентами из K, и трансцендентным в противном случае. Расширение L поля K называется алгебраическим, если всякий его элемент алгебраичен над K.*

Иными словами, элемент $a \in L$ алгебраичен над K, если он является корнем многочлена положительной степени с коэффициентами из поля K.

Теорема 4.21. *Конечное расширение является алгебраическим.*

Доказательство. Пусть $\dim_K L = n$ и $a \in L$. Тогда элементы $1, a, a^2, \ldots, a^n$ линейно зависимы над K. Следовательно, найдется их нетривиальная линейная комбинация равная нулю. Заменив a на x, получаем многочлен положительной степени с коэффициентами из поля K, корнем которого является элемент $a \in L$. □

Теорема 4.22. *Пусть $K < L < M$ – расширение полей, причем L – конечное расширение поля K, а M – конечное расширение поля L. Тогда M – конечное расширение поля K и $\dim_K M = \dim_K L \cdot \dim_L M$.*

Доказательство. Пусть $\langle e_1, \ldots, e_n \rangle$ – базис векторного пространства L над полем K и $\langle f_1, \ldots, f_m \rangle$ – базис векторного пространства M над полем L. Тогда утверждение будет доказано, если установить, что $\langle e_i f_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m \rangle$ есть базис векторного пространства M над полем K.

Произвольный элемент из M представляется линейной комбинацией векторов базиса $\langle f_1, \ldots, f_m \rangle$ с коэффициентами из поля L, а эти коэффициенты раскладываются по базису пространства L над K. Поэтому любой элемент из M является линейной комбинацией элементов $e_i f_j$ с коэффициентами из K. Если же $\sum\limits_{i,j} c_{ij} e_i f_j = 0$, где $c_{ij} \in K$, то поскольку $\sum\limits_{i,j} c_{ij} e_i f_j = \sum\limits_j (\sum\limits_i c_{ij} e_i) f_j$ и $\langle f_1, \ldots, f_m \rangle$ – базис M над полем L, получаем что $\sum_i c_{ij} e_i = 0$, откуда следует, что $c_{ij} = 0$ в силу того, что $\langle e_1, \ldots, e_n \rangle$ – базис L над полем K. Тем самым доказана полнота и линейная независимость над K системы $\langle e_i f_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m \rangle$. □

Пусть $K < L$ – расширение полей и $a \in L$ – алгебраический над K элемент. Отображение $\varphi : K[x] \to L$, $\varphi(f) := f(a)$ является гомоморфизмом с образом

$K[a] \subset L$. Ядро гомоморфизма φ – главный идеал, порожденный многочленом положительной степени со старшим коэффициентом 1, который мы обозначим как $m_a(x)$. Это – многочлен наименьший степени с коэфициентами в K, имеющий корень a в L. Его называют *минимальным многочленом элемента* a. Ясно, что $m_a(x)$ неприводим (иначе один из сомножителей имел бы тот же корень a, но меньшую степень). Из неприводимости, как мы видели выше, следует, что $K[a] \cong K[x]/(m_a(x))$ – поле, т.е. $K[a] = K(a)$. Напомним, что такое расширение называлось простым. Элемент a называют *примитивным*, а его *степенью* над K называют степень минимального многочлена m_a.

Предложение 4.23. *Конечное расширение L конечного поля K является простым.*

Доказательство. Возьмем образующую a циклической группы $L^* \cong \mathbb{Z}_{q-1}$, где $|L| = q = p^n$ и $p = \operatorname{char} K = \operatorname{char} K$. Тогда $L = \{0, a, a^2, \ldots, a^{q-1}\} = L^* \cup \{0\}$, т.е. $L = K[a] = \mathbb{F}_p[a] = \mathbb{F}_p(a) = K(a)$, и a – примитивный элемент. При этом, если $m_a(x) \in \mathbb{F}_p[x]$ (соответственно $\widetilde{m}_a(x) \in K[x]$) – минимальный многочлен элемента a над полем $\mathbb{F}_p$ (соответственно над K), то $L \cong \mathbb{F}_p[x]/(m_a(x)) \cong K[x]/(\widetilde{m}_a(x))$ и $\deg m_a(x) = n$, $\deg \widetilde{m}_a(x) = \dim_K L$. □

Кроме того, из доказательства предыдущего предложения видно, что для любого натурального $n \in \mathbb{N}$ существует неприводимый над $\mathbb{F}_p$ многочлен степени n, а также, что примитивными элементами в поле $\mathbb{F}_q$ являются образующие циклической группы $\mathbb{F}_q^* \cong \mathbb{Z}_{q-1} \cong C_{q-1}$ и только они. Число образующих равно $\varphi(q-1)$, где φ – функция Эйлера.

Соберем для удобства, полученные до сих пор факты, в следующую теорему.

Теорема 4.24. *Элемент $a \in L$ алгебраичен над K тогда и только тогда, когда $K[a]$ – конечномерная K-алгебра. Для алгебраического $a \in L$ алгебра $K[a]$ является полем, так что $K[a] = K(a)$ и степень расширения этого поля над K равна степени элемента a, т.е. равна степени минимального многочлена элемента a.*

Определение 4.25. *Расширение L поля K называется конечно порожденным, если $L = K(a_1, \ldots, a_n)$ для некоторого конечного набора элементов $a_1, \ldots, a_n \in L$.*

Теорема 4.26. *Следующие свойства расширения L поля K эквивалентны:*

1) L – конечное расширение,

2) L – конечно порожденное алгебраическое расширение,

3) L порождается над K конечным числом алгебраических элементов.

Доказательство. Пусть L над полем K порождается алгебраическим элементом $a \in L$, т.е. $L = K(a)$. Покажем, что расширение конечно, т.е. $\dim_K L < \infty$. Заметим, что $\dim_K K[a] < \infty$ в силу алгебраичности элемента a. Предположим противное. Тогда найдется бесконечная последовательность дробей $\frac{f_1(a)}{g_1(a)}, \frac{f_2(a)}{g_2(a)}, \ldots$, где $f_i(a), g_i(a)$ – многочлены от элемента a, такая, что любая конечная подсистема элементов из этой последовательности линейно независима над полем K. Умножив систему из первых n дробей на произведение их знаменателей $h_n = g_1 \cdot \ldots \cdot g_n$

получим систему из n многочленов от a, которая линейно независима. Поскольку n произвольно, получаем, что $K[a]$ бесконечномерно – противоречие.

Пусть $L = K(a_1, a_2)$, где a_1, a_2 – алгебраические элементы над полем K. Тогда a_2 является алгебраическим над $K(a_1)$, поскольку он является алгебраическим над меньшим полем $K \subset K(a_1)$. По доказанному $L = K(a_1, a_2) = K(a_1)(a_2)$ конечномерно над $K(a_1)$, а последнее конечномерно над K. Поэтому из предыдущей теоремы получаем требуемое – $\dim_K L = \dim_K K(a_1, a_2) < \infty$.

В общем случае пусть $L = K(a_1, \ldots, a_m)$, где $a_1, \ldots, a_m$ – алгебраические элементы над полем K. Тогда a_m является алгебраическим над $K(a_1, \ldots, a_{m-1})$, так как он является алгебраическим над меньшим полем $K \subset K(a_1, \ldots, a_{m-1})$. Следовательно, $L = K(a_1, \ldots, a_{m-1})(a_m)$ конечномерно над $K(a_1, \ldots, a_{m-1})$. Сделав индуктивное предположение, что $\dim_K K(a_1, \ldots, a_{m-1}) < \infty$, получаем из предыдущей теоремы, что $\dim_K L < \infty$. □

Теорема 4.27. *Пусть L – расширение поля K. Подмножество $\overline{K} \subset L$, состоящее из всех алгебраических над K элементов поля L, является подполем. Оно алгебраически замкнуто в L в том смысле, что любой элемент поля L, алгебраический над $\overline{K}$, принадлежит $\overline{K}$.*

Доказательство. Нужно доказать, что сумма, разность, произведение и частное двух алгебраических над K элементов поля L суть алгебраические над K элементы. Это так, поскольку $K(a, b) \subset \overline{K}$ для $a, b \in \overline{K}$.

Пусть $a \in L$ – алгебраический над $\overline{K}$ элемент. Тогда он является корнем многочлена $x^n + u_1 x^{n-1} + \cdots + u_{n-1}x + u_n$, где $u_1, \ldots, u_n \in \overline{K}$. Поэтому a – элемент алгебраический над полем $F := K(u_1, \ldots, u_n)$, а F является конечным расширением поля K в силу того, что элементы $u_1, \ldots, u_n$ являются алгебраическими над K. Поле $F(a)$ является конечным расширением поля F, поскольку a – алгебраический над F элемент. Следовательно, $F(u)$ – конечное расширение поля K и любой элемент поля $F(u)$ является алгебраическим над K, т.е. принадлежит $\overline{K}$. В частности, $a \in \overline{K}$. □

Поле $\overline{K}$ называют *алгебраическим замыканием поля K* в L.

Всякое конечное расширение поля $\mathbb{Q}$ называется *полем алгебраических чисел*. Всякое такое поле содержится в поле $\overline{\mathbb{Q}}$ – *поле всех алгебраических чисел*, которое определяется как замыканиии поля $\mathbb{Q}$ в $\mathbb{C}$.

Теорема 4.28. *Если F – конечное расширение над K, то F является простым расширением $F = K(u)$ для некоторого элемента u, называемого примитивный элементом, тогда и только тогда, когда F имеет конечное число промежуточных полей.*

Эта теорема верна, если K – конечное поле, поэтому предположим, что K бесконечно. Пусть F над K имеет конечное число промежуточных полей. Выберем u в F так, чтобы размерность $K(u)$ над K была максимальной. Предположим, что $K(u)$ остается собственным подполем в F, и возьмем какой-нибудь $v \in F \setminus K(u)$. Рассмотрим все промежуточные поля $K(u + av)$, где a берется из K. Поскольку K бесконечно, должны существовать два разных элемента a и b поля K такие, что

$K(u+av) = K(u+bv)$. Отсюда следует, что $(u+av)-(u+bv) = (a-b)v$ лежит в $K(u+av)$. Разделив на $a-b$ видим, что $v \in K(u+av)$. Умножив v на a и вычтя из $u+av$, получаем, что $u \in K(u+av)$. Таким образом, $K(u+av)$ содержит $K(u,v)$. Но тогда $\dim_K K(u+av) > \dim_K K(u)$ так как $v \notin K(u)$, а это противоречит выбору элемента u. Полученное противоречие говорит о том, что должен быть некоторый u такой, что $K(u) = F$, т.е. F – простое расширение с примитивным элементом u.

Обратно, предположим, что $F = K(u)$. Пусть u – корень неприводимого многочлена $p(x)$ со старшим коэффициентом 1. Если E – промежуточное расширение, разложим $p(x)$ на множители в E и найдем такой неприводимый множитель $q(x)$, для которого u является корнем, т.е. $q(u) = 0$. Присоединив коэффициенты многочлена q к K, получим подполе в E, которое обозначим через L. Конечно, q остается неприводимым над L, и по-прежнему $q(u) = 0$. Размерность $L(u)$ над L – это степень многочлена q. Размерность $E(u)$ над E также является степенью q, а $L(u)$ и $E(u)$ оба равны F. Следовательно, E и L имеют одинаковую размерность над K, а поскольку одно содержит другое, они равны. Таким образом, подполе E порождается коэффициентами неприводимого многочлена $q(x)$.

Многочлен $p(x)$ разлагается в произведение нормированных неприводимых многочленов в кольце $F[x]$. Эти неприводимые многочлены объединяются конечным числом способов для построения промежуточных многочленов $q(x)$. Следовательно, существует конечное число промежуточных полей.

Теорема 4.29. *Всякое конечное расширение поля нулевой характеристики является простым.*

4.3 Поле частных области целостности

Поле частных, называемое также полем отношений, – это наименьшее поле, в которое погружается область целостности. Пусть R – область целостности. Если R содержится в поле L как подкольцо так, что единицы $1 \in R$ и $1 \in L$ совпадают, то определены элементы $b^{-1}a = ab^{-1}$, $b \neq 0$, $a, b \in R \subset L$. Если эти элементы записывать как дроби $a/b = \frac{a}{b}$, то правила сложения, умножения и деления не будут отличаться от тех же правил обращения с обычными дробями (отношениями целых чисел, многочленов и пр.).

Построение поля частных

Пусть R – области целостности. На множестве пар a, b, где $a, b \in R \subset L$ и $b \neq 0$, определим отношение эквивалентности по правилу

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 b_2 = a_2 b_1.$$

Рефлексивность и симметричность очевидны. Транзитивность: пусть $(a_1, b_1) \sim (a_2, b_2)$, $(a_2, b_2) \sim (a_3, b_3)$, тогда

$$a_1 b_2 = a_2 b_1 \;\Rightarrow\; a_1 b_2 b_3 = a_2 b_1 b_3, \qquad a_2 b_3 = a_3 b_2 \;\Rightarrow\; a_2 b_3 b_1 = a_3 b_2 b_1,$$

откуда $a_1b_2b_3 = a_3b_2b_1$, и сокращая на b_2, получаем $a_1b_3 = a_3b_1$, т.е. $(a_1, b_1) \sim (a_3, b_3)$.

Итак, у нас есть отношение эквивалентности и мы можем взять фактормножество. Заметим, что в этом фактормножестве класс пары и не изменится, если ее умножить на ненулевой элемент кольца, поскольку $(a, b) \sim (ac, bc)$, $c \neq 0$.

Чтобы определить операции сложения и умножения в фактормножестве определим сначала операции на парах:

$$(a_1, b_1) + (a_2, b_2) = (a_1b_2 + a_2b_1, b_1b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2).$$

Проверяется, что эти операции согласованы с введенным отношением эквивалентности, и, тем самым, в фактормножестве появляется сложение и умножение, причем по отношению к этим операциям фактормножество является ассоциативным и коммутативным кольцом. Нулем служит класс пары $(0, b)$, $b \neq 0$, а единицей класс любой пары вида (a, a), $a \neq 0$. Далее видно, что если $a \neq 0$, $b \neq 0$, то класс пары (b, a) обратен к классу пары (a, b). Таким образом, мы имеем поле. Его обозначают через $\operatorname{Quot} R$ и называют полем частных области целостности R. Кольцо R вкладывается в свое поле частных очевидным образом – элементу $a \in R$ сопоставляется класс пары $(a, 1)$. Классы пар, т.е. элементы поля частных, удобно представлять дробями $a/b = \frac{a}{b}$. В этих обозначениях сложение, умножение и деление осуществляется по правилам обращения с обычными дробями.

Если R — область целостности, множество всех его ненулевых элементов образует мультипликативную систему.

Определение 4.30. *Подмножество S кольца с единицей называется мультипликативной системой, если оно содержит единицу, не содержит нуля и замкнуто по умножению.*

Кольцо частных целостного кольца R по этой системе (т.е. по системе $S = R \setminus \{0\}$) является полем и называется полем частных или полем отношений, оно обычно обозначается $\operatorname{Quot} R$. Все элементы поля частных имеют вид a/b, где a, b – элементы R и $b \neq 0$, с обычными арифметическими правилами сокращения числителя и знаменателя, сложения и умножения.

Легко видеть, что поле частных – наименьшее поле, в которое можно вложить R. Например, поле частных поля изоморфно самому полю.

Область целостности естественным образом вкладывается в свое поле частных при отображении $a \mapsto a/1$. Поле частных целостного кольца R удовлетворяет следующему универсальному свойству: если $\varphi : R \to F$ — инъективный гомоморфизм колец из R в поле F, то существует единственный гомоморфизм колец $\psi : \operatorname{Quot} R \to F$, который совпадает с φ на элементах кольца R.

Примеры 4.31. 1. $\operatorname{Quot} \mathbb{Z} = \mathbb{Q}$.

2. $\operatorname{Quot} K[x] = K(x)$ – поле рациональных функций, т.е. полем частных кольца многочленов над полем K является поле рациональных функций, состоящее из всевозможных отношений многочленов $f(x)/g(x)$, $f, g \in K[x]$.

3. Полем частных кольца формальных степенных рядов $K[[x]]$ над полем K является поле рядов Лорана. Элементы ряда Лорана – это формальные степенные

ряды деленные на x^n, $n = 0, 1, \ldots$, их можно представлять себе как формальный ряд Лорана:

$$\frac{a_{-n}}{x^n} + \cdots + \frac{a_{-1}}{x} + a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k + \ldots,$$

где коэффициенты a_j взяты из поля K. Если $K = \mathbb{C}$ и ряд сходится в проколотой окрестности точки $0 \in \mathbb{C}$, то при $a_{-n} \neq 0$ такой ряд представляет собой обычный ряд Лорана функции, имеющей в нуле полюс порядка n.

В терминах теории категорий конструкцию поля частных можно описать следующим образом. Рассмотрим категорию, объекты которой — целостные кольца, а морфизмы – инъективные гомоморфизмы колец. Существует забывающий функтор из категории полей в эту категорию (так как все гомоморфизмы полей инъективны). Оказывается, что у этого функтора существует левый сопряженный, он и сопоставляет целостному кольцу его поле частных.

4.4 Локализация кольца (кольцо частных)

Кольцом частных $S^{-1}R$ коммутативного кольца R с единицей по мультипликативной системе $S \subset R$ называется пространство дробей с числителями из R и знаменателями из S с арифметическими операциями и отождествлениями, обычными для дробей. Используется также термин *локализация кольца* R по множеству S.

Мультипликативной системой в кольце R называется подмножество S в R, содержащее 1, не содержащее нуля и замкнутое по умножению в кольце R. Для мультипликативной системы S множество $I_S = \{a \in R : \exists s \in S,\ as = 0\}$ образует идеал в кольце R. В случае, когда множество S не содержит делителей нуля кольца R, идеал I_S состоит только из нуля и система S называется *регулярной*. В целостном кольце всякая мультипликативная система регулярна.

Элементами кольца частных кольца R по мультипликативной системе S являются формальные дроби вида r/s, где $r \in R$, а $s \in S$. Две дроби r_1/s_1 и r_2/s_2 считаются эквивалентными (представляют один и тот же элемент кольца частных), если $r_1 s_2 - r_2 s_1 \in I_S$. Операции сложения и умножения определяются как обычно:

$$r_1/s_1 + r_2/s_2 = (r_1 s_2 + r_2 s_1)/s_1 s_2,$$
$$r_1/s_1 \cdot r_2/s_2 = r_1 r_2/s_1 s_2.$$

Проверяется, что, если в сумме или произведении дроби заменить на эквивалентные, новый результат будет выражаться дробью, эквивалентной прежней. С такими операциями множество $S^{-1}R$ приобретает структуру коммутативного кольца с единицей. Нулём в нём служит дробь $0/1$, единицей — дробь $1/1$.

Если к определению подходить более формально, то так же как при определении поля частных целостного кольца нужно определить подходящее отношение эквивалентности – в данном случае на множестве пар из $R \times S$. Полагаем $(r_1, s_1) \sim (r_2, s_2)$, если найдется элемент $s \in S$ такой, что $s(r_1 s_2 - r_2 s_1) = 0$. Класс пары (r, s) удобно представлять себе как дробь $r/s = \frac{r}{s}$. Проверяется, что определенные выше операции сложения и умножения (переписанные в обозначениях пар элементов) согласованы

и отношением эквивалентности и, тем самым, возникают корректно определенные операции на элементах фактормножества. В результате имеем кольцо $S^{-1}R$, которое ассоциативно, коммутативно и имеет единицу.

Свойства

Кольцо частных имеет каноническую структуру алгебры над кольцом R, так как вместе с кольцом $S^{-1}R$ сразу определен и канонический гомоморфизм кольца R в $S^{-1}R$ (каждому элементу r из R соответствует дробь $r/1$). Ядром этого гомоморфизма является идеал I_S. В случае, если система S *регулярна* – не содержит делителей нуля, этот гомоморфизм инъективен, и кольцо R, таким образом, вложено в свое кольцо частных по системе S. При этом дробь r/s является единственным решением уравнения $sx = r$. Если оба элемента r и s принадлежат S, тогда в кольце $S^{-1}R$ содержатся дроби r/s и s/r. Их произведение равно 1, следовательно, они обратимы. Обратно: каждый обратимый элемент кольца $S^{-1}R$ имеет вид er/s, где r и s принадлежат S, а e – обратимый элемент кольца R.

Если система S состоит из одних только обратимых элементов кольца R, канонический гомоморфизм кольца R в $S^{-1}R$ превращается в изоморфизм, так как каждая дробь r/s оказывается сократимой в кольце R.

Если R — область целостности, множество $S = R \setminus \{0\}$ всех его ненулевых элементов образует мультипликативную систему. Кольцо частных по этой системе – это поле частных (или поле отношений) $\operatorname{Quot} R$.

Вместо обозначения $S^{-1}R$ для локализации (или кольца частных) в отдельных случаях чаще употребляют другие обозначения. Так, если S – дополнение простого идеала I (определение простого идеала дается ниже), локализация R обозначается как R_I и называется локализацией кольца по простому идеалу, а если S – множество всех степеней элемента f, используется обозначение R_f.

Примеры 4.32. 1. Полем частных кольца целых чисел $\mathbb{Z}$ по мультипликативной системе, состоящей из нечетных чисел, будет кольцо рациональных дробей, у которых в несократимом виде знаменатель является нечетным числом.

2. Степени числа 10 в $\mathbb{Z}$ образуют мультипликативную систему. Кольцом частных по ней будет кольцо конечных десятичных дробей.

Пусть M – R-модуль, и S – мультипликативнное подмножество в R. Определим локализацию $S^{-1}M$ как множество дробей m/s, где $m \in M$, $s \in S$. Считаем, что m/s и m'/s' определяют один и тот же элемент в $S^{-1}M$, если существует $s'' \in S$ такой, что $s''(s'm - sm') = 0$.

Замечание 4.33. *Операция S^{-1} является функтором, причем точным.*

4.5 Максимальные и простые идеалы

Для того, чтобы доказывать существование максимального идеала в кольце (определение ниже), нам потребуется принять в качестве аксиомы так называему аксиому выбора, а точнее, лемму Цорна, которая ей эквивалентна.

Напомним понятия связанные с порядком.

Пусть на множестве X задан порядок, т.е. задано отношение $\leq$, определенное на некотором подмножестве пар в $X \times X$. Множество называется *частично упорядоченным*, если отношение $\leq$ рефлексивно, транзитивно и антисимметрично, т.е.

1. $x \leq x$ (рефлексивность);

2. если $x \leq y$ и $y \leq z$, то $x \leq z$ (транзитивность);

3. если $x \leq y$ и $y \leq x$, то $x = y$ (антисимметричность).

Строгое неравенство $<$ вводится очевидным образом: $x < y$ если $x \leq y$ и $x \neq y$. Кроме того, удобно договориться писать $y \geq x$, если $x \leq y$.

Если для элементов $x, y \in X$ верно $x \leq y$ или верно $y \leq x$, то элементы x и y называются сравнимыми. Элементы $x, y \in X$, не являющиеся сравнимыми, называются несравнимыми. Если все пары элементов множества X сравнимы относительно порядка $\leq$, то порядок $\leq$ называется *линейным*. Множество X с заданным на нем частичным порядком $\leq$ называется *частично упорядоченным множеством*. Если частичный порядок $\leq$ является линейным, то X называется *линейно упорядоченным множеством*.

Линейно упорядоченное подмножество в частично упорядоченном множестве называется *цепью* (на подмножестве рассматривается порядок, индуцированный порядком рассматриваемого частично упорядоченного множества).

АКСИОМА ВЫБОРА. *Для всякого семейства непустых множеств существует функция, называемая функцией выбора для заданного семейства, которая каждому множеству из семейства сопоставляет один из элементов этого множества.*

По другому: если X_i непустое множество для каждого $i \in A$, то декартово произведение $\Pi_{i \in A} X_i$ непусто.

Лемма 4.34 (Лемма Цорна)**.** *Частично упорядоченное множество, в котором любая цепь имеет верхнюю грань, содержит максимальный элемент.*

Верхняя грань цепи – это элемент больше либо равный любого элемента цепи. Элемент *максимален*, если не существует большего, чем он элемента.

Существует несколько альтернативных формулировок леммы Цорна.

В оригинальной статье 1935 года Цорн сформулировал утверждение для множеств, частично упорядоченных по отношению включения:

Если семейство множеств $\mathfrak{M}$ обладает тем свойством, что объединение любой цепи множеств из $\mathfrak{M}$ есть снова множество из этого семейства, то $\mathfrak{M}$ содержит максимальное множество.

Именно эта формулировка нам и понадобится для доказательства существования максимальных идеалов в любом кольце.

Еще одна эквивалентная формулировка – это теорема Цермело, утверждающая, что *каждое множество может быть вполне упорядочено.*

Вполне упорядоченное множество – это линейно упорядоченное множество, в котром каждое его непустое подмножество имеет минимальный элемент, т.е. элемент меньший либо равный любого элемента подмножества.

Задача 4.35. 1. Докажите, что у любого линейного пространства есть базис.

2. Пусть A – абелева группа, B – ее подгруппа, D – делимая абелева группа. Докажите, что любой гомоморфизм из B в D продолжается до гомоморфизма из A в D.

Для любого кольца R само R и нулевой идеал 0 являются идеалами (двусторонними). Такие идеалы называются тривиальными. Собственные идеалы — это идеалы, образующие собственное подмножество, то есть не совпадающие со всем R.

Теперь мы можем ввести понятие максимального идеала.

Определение 4.36. *Идеал I кольца R называется максимальным, если он является максимальным по включению среди всех собственных идеалов кольца R.*

Теорема 4.37. *В любом ассоциативном кольце R с единицей существует (возможно, не единственный), максимальный идеал I. Любой собственный идеал содержится в максимальном идеале.*

Доказательство. Мы воспользуемся следующим очевидным утверждением: Идеал I кольца R не совпадает со всем кольцом R тогда и только тогда, когда он не содержит единицы.

Теперь перейдем к доказательству теоремы. Рассмотрим множество всех идеалов кольца R отличных от R с отношением порядка по включению. Оно непусто, так как содержит нулевой идеал. Если в этом множестве есть некоторая линейно упорядоченная цепь идеалов, то она состоит из вложенных друг в друга идеалов. Взяв ее объединение, мы снова получим идеал, отличный от R, так как объединение не содержит единицы. Значит, множество собственных идеалов удовлетворяет условию леммы Цорна, т.е. обладает некоторым максимальным элементом, который и есть максимальный идеал I.

Второе утверждение доказывается таким же образом, но вместо нулевого идеала берем множество всех собственных идеалов, содержащих данный собственный идеал. Это множество непусто, поскольку содержит заданный идеал. Дальнейшие рассуждения повторяют приведенные выше. □

Теорема 4.38. *Идеал I кольца R является максимальным тогда и только тогда, когда R/I – поле.*

Доказательство. Идеалу кольца R/I соответствует его прообраз в кольце R. Этот прообраз является идеалом в R. Действительно, пусть $\pi : R \to R/I$ – канонический эпиморфизм на фактор, I' – идеал в R/I и $J := \pi^{-1}I'$. Ясно, что J содержит I, и является аддитивной подгруппой в R. Возьмем $r \in R$ и $s \in J$, $\pi(rs) = \pi(r)\pi(s) = (r + I)(s + I) \in I'$, поскольку второй сомножитель лежит в I', а I' – идеал в R/I.

Наоборот, идеалу J, содержащему I, соответствует подмножество $I' := \pi(J) \subset R/I$. Поскольку π – гомоморфизм (колец и R-модулей).

Тем самым, доказано следующее утверждение: имеется взаимно однозначное соответствие между идеалами кольца R/I и идеалами кольца R, содержащими идеал I.

Теперь, если R/I – поле, то I максимален, поскольку образ любого собственного идеала $J \lhd R$, содержащего I, есть собственный идеал в поле R/I, т.е. нулевой идеал,

поскольку в поле есть всего два идеала (нулевой и само поле). Последнее означает, что $J = I$.

Если I максимален, то идеал, содержащий $r \in R \setminus I$ и I совпадает с R. Следовательно, $(r) + I = R$, поэтому существует элемент $r' \in R$ такой, что $rr' \in 1 + I$, откуда получаем $(r + I)(r' + I) = 1 + I$, а это означает, что элемент $r + I$ обратим в R/I, т.е. R/I – поле. □

Определение 4.39. *Идеал I в кольца A называется простым, если факторкольцо A/I по нему является областью целостности.*

Равносильная формулировка: *если $I \neq A$ и из $ab \in I$ следует $a \in I$ или $b \in I$, то I – простой идеал.*

Идеал I прост тогда и только тогда, когда элементы дополнения к нему образуют мультипликативную систему.

Максимальный идеал кольца, т.е. собственный идеал, не содержащийся ни в каком собственном идеале, является простым, поскольку фактор по максимальному идеалу – поле, а поле является областью целостности.

Максимальные идеалы в кольце $\mathbb{Z}$ целых чисел – это идеалы вида $(p) = p\mathbb{Z}$, где p – простое число. Простые идеалы в $\mathbb{Z}$ – это все максимальные идеалы плюс нулевой идеал.

Идеалу кольца R/I соответстует его прообраз в кольце R. Этот прообраз является идеалом в R. Действительно, пусть $\pi : R \to R/I$ – канонический эпиморфизм на фактор, I' – идеал в R/I и $J := \pi^{-1}I'$. Ясно, что J содержит I, и является аддитивной подгруппой в R. Покажем, что J – идеал в R. Возьмем $r \in R$ и $s \in J$, тогда $\pi(rs) = \pi(r)\pi(s) = (r + I)(s + I) \in I'$, поскольку второй сомножитель лежит в I', а I' – идеал в R/I. Следовательно, $rs \in \pi^{-1}I' = J$.

Наоборот, идеалу J, содержащему I, соответствует подмножество $I' := \pi(J) \subset R/I$. Поскольку π – гомоморфизм (колец и R-модулей), I' – идеал в R/I.

Тем самым, доказано следующее утверждение:

Предложение 4.40. *Имеется взаимно однозначное соответствие между идеалами кольца R/I и идеалами кольца R, содержащими идеал I.*

Теорема 4.41. *Идеал I кольца R является максимальным тогда и только тогда, когда R/I – поле.*

Доказательство. Теперь, если R/I – поле, то I максимален, поскольку образ любого собственного идеала $J \triangleleft R$, содержащего I, есть собственный идеал в поле R/I, т.е. нулевой идеал, поскольку в поле есть всего два идеала (нулевой и само поле). Последнее означает, что $J = I$.

Если I максимален, то идеал, содержащий $r \in R \setminus I$ и I совпадает с R. Следовательно, $(r) + I = R$, поэтому существует элемент $r' \in R$ такой, что $rr' \in 1 + I$, откуда получаем $(r + I)(r' + I) = 1 + I$, а это означает, что элемент $r + I$ обратим в R/I, т.е. R/I – поле. □

Определение 4.42. *Идеал I в кольца A называется простым, если факторкольцо A/I по нему является областью целостности.*

Равносильная формулировка: *если $I \neq A$ и из $ab \in I$ следует $a \in I$ или $b \in I$, то I – простой идеал.*

Идеал I прост тогда и только тогда, когда элементы дополнения к нему образуют мультипликативную систему.

Максимальный идеал кольца, т.е. собственный идеал, не содержащийся ни в каком собственном идеале, является простым, поскольку фактор по максимальному идеалу – поле, а поле является областью целостности.

Максимальные идеалы в кольце $\mathbb{Z}$ целых чисел – это идеалы вида $(p) = p\mathbb{Z}$, где p – простое число. Простые идеалы в $\mathbb{Z}$ – это все масимальные идеалы плюс нулевой идеал.

Аналогично, в кольце многочленов $K[x]$ над полем максимальный идеал – это главный идеал, порожденный неприводимым многочленом, поскольку факторкольцо по такому идеалу есть поле, а простые идеалы – это все масимальные идеалы плюс нулевой идеал.

Если элемент кольца не обратим, тогда все элементы кольца, кратные ему, образуют главный идеал, порожденный этим элементом, и этот главный идеал является собственным, и, значит, лежит в некотором максимальном.

Предложение 4.43. *Каждый необратимый элемент кольца содержится в некотором максимальном идеале.*

Предложение 4.44. *В области главных идеалов любой ненулевой простой идеал максимален.*

Доказательство. Напомним, что областью главных идеалов называется область целостности (или – целостное кольцо = ассоциативное, коммутативное кольцо с 1 и без делителей нуля), в котором каждый идеал главный. Пусть $0 \neq (x)$ – простой идеал в R. Предположим, что он строго содержится в идеале (y). Тогда $x \in (y) \;\Rightarrow\; x = yz \in (x)$. Так как $y \notin (x)$ и (x) – простой идеал, получаем, что $z \in (x)$, откуда $z = tx$. Далее,

$$x = yz = ytx \;\Rightarrow\; x(1 - yt) = 0 \;\Rightarrow\; yt = 1 \;\Rightarrow\; (y) = R.$$

Сокращение на x законно, поскольку R – целостное кольцо. □

Если элемент обратим, то всякий идеал, который его содержит, совпадает со всем кольцом, поэтому обратимые элементы не содержатся ни в каком собственном идеале, соответственно и ни в каком максимальном. Если все необратимые элементы кольца R образуют идеал, он является максимальным, и притом единственным – других максимальных идеалов в кольце R нет. Верно и обратное: если в кольце R максимальный идеал единствен, он включает в себя все необратимые элементы кольца.

Определение 4.45. *Кольцо с единственным максимальным идеалом называется локальным.*

Определение 4.46. *Если R – локальное кольцо и $\mathfrak{m}$ – его единственный максимальный идеал, то поле $R/\mathfrak{m}$ называется полем вычетов кольца R.*

Примеры 4.47. 1. Максимальным идеалом в поле является нулевой идеал. В частности, поле является локальным кольцом.

2. Максимальными идеалами в кольце целых чисел являются идеалы $p\mathbb{Z} = (p)$, где p простое. Например, чётные числа образуют максимальный идеал, а числа, кратные 4 – образуют идеал, но не максимальный – этот идеал содержится в идеале четных чисел.

3.Максимальными идеалами в кольце многочленов $K[x]$ над полем K являются главные идеалы, порожденные неприводимыми многочленами. Поэтому кольцо $K[x]$ не является локальным кольцом.

4. Максимальными идеалами в кольце Z_n являются идеалы, порожденные простыми числами, делящими n. В частности, кольцо $\mathbb{Z}_{p^n}$, где p простое, является локальным кольцом.

5. В кольце рядов $K[[x]]$ над полем K единственным максимальным идеалом является идеал (x). Таким образом, $K[[x]]$ является локальным кольцом. Ряд, у которого свободный член не равен нулю обратим, поэтому необратимые элементы – те, которые не содержат свободного члена. Они и образуют единственный максимальный идеал (x).

6. В прямой сумме колец $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ максимальными идеалами являются $R_1 \oplus \cdots \oplus R_{i-1} \oplus I_i \oplus R_{i+1} \oplus \cdots \oplus R_n$, где I_i – максимальный идеал в R_i.

7. В кольце многочленов $K[X, Y]$, где K - алгебраически замкнутое поле, максимальные идеалы имеют вид $I_{a,b} = \{f \in K[X, Y] : f(a, b) = 0\}, \quad a, b \in K$.

Задача 4.48. Докажите, что максимальными идеалами в кольце матриц $M_{n\times n}(R)$ над кольцом R являются кольца матриц $M_{n\times n}(I)$ над максимальными идеалами I кольца R.

Определение 4.49. *Элемент x кольца R называется нильпотентным, если существует натуральное n, такое, что $x^n = 0$. Минимальное значение n, для которого справедливо это равенство, называется индексом нильпотентности элемента x.*

Лемма 4.50. *Сумма и разность двух нильпотентных элементов нильпотентна, как и произведение нильпотентного и произвольного элементов.*

Доказательство. Если $a^n = 0$, то $(ra)^n = r^n a^n = r^n \cdot 0 = 0$.

Пусть N – наибольший из индексов нильпотентности элементов $a, b \in R$. Тогда $a^N = b^N = 0$, и по формуле бинома получаем

$$(a + b)^{2N} = \sum_{i+j=2N} C_{2N}^i a^i b^j = 0.$$

Сумма равна нулю, поскольку тривиально каждое слагаемое, так как либо $i \geq N$, либо $j \geq N$. □

Из этой леммы следует, что совокупность всех нильпотентных элементов является идеалом.

Определение 4.51. *Нильрадикалом* $\operatorname{Rad} R$ *коммутативного кольца R называется идеал, состоящий из всех его нильпотентных элементов.*

Предложение 4.52. *Факторкольцо по нильрадикалу не содержит нетривиальных нильпотентов.*

Доказательство. Обозначим через π канонический эпиморфизм кольца R на его факторкольцо по нильрадикалу. Пусть $\pi(r)$ – нильпотент. Тогда $(\pi(r))^n = 0$ для некоторого $n \in \mathbb{N}$. Следовательно, $0 = (\pi(r))^n = \pi(r^n)$, и, значит, $r^n \in \operatorname{Rad} R$. Поэтому найдется натуральное m, что

$$(r^n)^m = 0 \;\Rightarrow\; r^{nm} = 0 \;\Rightarrow\; r \in \operatorname{Rad} R \;\Rightarrow\; \pi(r) = 0.$$

□

Теорема 4.53. *Пересечение всех простых идеалов совпадает с нильрадикалом.*

Доказательство. Обозначим через T пересечение всех простых идеалов кольца R. Пусть I – простой идеал и $a \in R$ – нильпотент, т.е. $a^n = 0 \in I$. Отсюда следует, что $a \in I$. Действительно, поскольку $a^n = a \cdot a^{n-1}$, из простоты идеала I следует, что либо $a \in I$, либо $a^{n-1} \in I$. Во втором случае, представляем $a^{n-1} = a \cdot a^{n-2}$ и пользуемся тем же соображением. В результате получим, что $a \in I$. Следовательно, a принадлежит любому простому идеалу, а, значит, и их пресечению.

Пусть теперь a не является нильпотентом. Покажем, что $a \notin T$. Обозначим через Σ множество всех таких идеалов I в R, что при любом $n \in \mathbb{N}$ выполнено $a^n \notin I$. Оно непусто, поскольку содержит нулевой идеал. Введем порядок на Σ по включению идеалов. Рассмотрим цепь в Σ. Объединение идеалов цепи будет идеалом, принадлежащим Σ, и этот идеал есть верхняя грань цепи. Поэтому выполнены условия леммы Цорна, и, следовательно, в Σ имеется максимальный элемент, который обозначим через $\mathfrak{p}$. Пусть $x, y \notin \mathfrak{p}$. Тогда идеалы $\mathfrak{p} + (x)$ и $\mathfrak{p} + (y)$ строго содержат идеал $\mathfrak{p}$, и поэтому не принадлежат Σ. Последнее означает, что существуют натуральные n, m такие, что $a^m \in \mathfrak{p} + (x)$ и $a^n \in \mathfrak{p} + (y)$. Поэтому $a^{m+n} \in \mathfrak{p} + (xy)$, откуда следует, что идеал $\mathfrak{p} + (xy)$ не принадлежит Σ, так что $xy \notin \mathfrak{p}$. Таким образом, нами построен простой идеал $\mathfrak{p}$, не содержащий a, поэтому $a \notin T$. □

Если $A, B \subset R$ – два подмножества кольца R, то их произведением $A \cdot B = AB$ называется подмножество в R, состоящее из сумм (конечных) всевозможных произведений ab, $a \in A$, $b \in B$. Суммой $A + B$ называется множество элементов вида $a + b$, $a \in A$, $b \in B$.

В частности, определены суммы и произведения идеалов, а также степень идеала (как частный случай произведения). Это будут, как легко проверить, идеалы в R.

Определение 4.54. *Идеал I коммутативного кольца R называется нильпотентным, если $I^n = 0$.*

Предложение 4.55. *Если нильрадикал конечно порожден, то он нильпотентен.*

Доказательство. Предположим, что $\operatorname{Rad} R$ порождается элементами $a_1, \ldots, a_s$. Тогда любой элемент нильрадикала можно представить как $r_1 a_1 + \cdots + r_s a_s$. Пусть

N – наибольший из индексов нильпотентности элементов $a_1, \ldots, a_s$. Тогда индекс нильпотентности элемента $r_i a_i$ тоже не превосходит N. Поэтому индекс нильпотентности элемента $r_1 a_1 + \cdots + r_s a_s$ не будет превосходить Ns, откуда следует, что нильрадикал возведенный в степень Ns, равен нулю. Действительно, $(r_1 a_1 + \cdots + r_s a_s)^{Ns}$ равен линейной комбинации (с коэффициентами в R) элементов вида $a_1^{i_1} \cdot \ldots \cdot a_s^{i_s}$ с $i_1 + \cdots + i_s = Ns$. Последнее равенство влечет неравенство $i_j \geq N$ для некоторого j, и тогда $a_j^{i_j} = 0$. □

Определение 4.56. *Радикалом Джекобсона называется пересечение всех максимальных идеалов кольца.*

Каждый максимальный идеал прост, поэтому радикал Джекобсона содержит нильрадикал.

Предложение 4.57. *Элемент $x \in R$ принадлежит радикалу Джекобсона в том и только том случае, когда элемент $1 - xy$ обратим в R для всех $y \in R$.*

Доказательство. Если $1 - xy$ не является обратимым, то он принадлежит некоторому максимальному идеалу $\mathfrak{m}$, но поскольку $x \in R$ принадлежит радикалу Джекобсона (пересечению всех максимальных идеалов), то $x \in \mathfrak{m} \;\Rightarrow\; xy \in \mathfrak{m}$. Откуда получаем $1 \in \mathfrak{m}$, т.е. $R = \mathfrak{m}$ – противоречие (максимальный идеал является собственным).

Обратно, пусть $x \notin \mathfrak{m}$, где $\mathfrak{m}$ – некоторый максисмальный идеал. Тогда $\mathfrak{m} + (x) = R$, поэтому найдутся $u \in \mathfrak{m}$ и $y \in R$ такие, что $u + xy = 1 \;\Rightarrow\; 1 - xy \in \mathfrak{m}$, поэтому $1 - xy$ не является обратимым. □

Определение 4.58. *Радикалом идеала I называется*

$$\sqrt{I} = r(I) := \{a \in R \mid \exists\, n \in \mathbb{N} :\; a^n \in I\}.$$

Эквивалентное определение радикала идеала I – это прообраз нильрадикала кольца R/I при отображении факторизации. Это также доказывает, что $\sqrt{I}$ является идеалом.

Теорема 4.59. *Пересечение всех простых идеалов, содержащих идеал I, совпадает с радикалом идеала I.*

Доказательство. Прообраз при гомоморфизме любого простого идеала прост. Мы знаем, что нильрадикал кольца R/I является пересечением простых идеалов. Беря прообраз этих простых идеалов, видим, что I является их пересечением. □

Примеры

1. В кольце целых чисел радикал главного идеала $(n) = n\mathbb{Z}$ – это главный идеал, порожденный произведением всех простых делителей числа n, т.е. если $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ – произведение степеней простых чисел $p_1, \ldots, p_s$, то радикал главного идеала (n) есть идеал $(p_1 \cdot \ldots \cdot p_s) = p_1 \cdot \ldots \cdot p_s \mathbb{Z}$.

2. $\operatorname{Rad} \mathbb{Z}_n = (p_1 \cdot \ldots \cdot p_s) = p_1 \cdot \ldots \cdot p_s \mathbb{Z}_n$, если $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$.

Например, $\operatorname{Rad} \mathbb{Z}_{20} = (10)$, $\mathbb{Z}_{20}/(10) \cong \mathbb{Z}_{10}$.

3. В любом коммутативном кольце $\sqrt{\mathfrak{p}^k} = \mathfrak{p}$ для простого идеала $\mathfrak{p}$. В частности, каждый простой идеал *радикален*, т.е. совпадает со своим радикалом.

Свойства

$\sqrt{\sqrt{I}} = \sqrt{I}$. Более того, $\sqrt{I}$ — это наименьший радикальный идеал, содержащий идеал I. В частности, нильрадикал — это пересечение всех простых идеалов.

Идеал является радикальным тогда и только тогда, когда факторкольцо по нему не содержит нетривиальных нильпотентов.

Если отличный от нуля элемент $a \in R$ кольца R является нильпотентом, то он является делителем нуля. Действительно, если n – индекс нильпотентности элемента a, то $a^n = 0$ и $a^{n-1} \neq 0$, поэтому равенство $0 = a^n = a \cdot a^{n-1}$ говорит о том, что a и a^{n-1} – делители нуля. Из этого утверждения немедленно следует, что:

Нильрадикал целостного кольца равен нулевому идеалу.

В частности, нильрадикал тривиален у полей и колец $\mathbb{Z}$, $R[x]$, $R[[x]]$, где R – целостное кольцо.

Рассмотрим сумму колец $R = R_1 \oplus \cdots \oplus R_s$. Если элемент $(a_1, \ldots, a_s) \in R$ является нильпотентом, то каждый из элементов a_i – нильпотент и наоборот. Поэтому $\operatorname{Rad} R = \operatorname{Rad} R_1 \oplus \cdots \oplus \operatorname{Rad} R_s$ и $R/\operatorname{Rad} R = R_1/\operatorname{Rad} R_1 \oplus \cdots \oplus R_s/\operatorname{Rad} R_s$.

Найдем нильрадикал кольца $\mathbb{Z}_{p^k}$, где p – простое число. В этом кольце (как и в любом кольце $\mathbb{Z}_n$) любой идеал является главным (при этом если n не является простым числом). Действительно, мы видели, что идеалы в $\mathbb{Z}_{p^k}$ однозначно соответствуют идеалам в $\mathbb{Z}$, содержащим идеал $\mathbb{Z}_{p^k}$. Биекция определяется следующим образом: идеалу кольца $\mathbb{Z}_{p^k}$ ставится в соответствие его прообраз при каноническом эпиморфизме $\pi : \mathbb{Z} \to \mathbb{Z}_{p^k}$ на факторкольцо. Так как $\mathbb{Z}$ – кольцо главных идеалов, прообраз $\pi^{-1}(I)$ любого идеала $I \lhd \mathbb{Z}_{p^k}$ есть главный идеал $(m) \lhd \mathbb{Z}$, содержащий идеал (p^k), откуда следует, что $m | p^k$, т.е. $m = p^l$ с $l \leq k$. При этом $\pi(m\mathbb{Z}) = I$, что можно записать как $I = m\mathbb{Z}_{p^k}$. Рассмотрим композицию гомоморфизмов $\mathbb{Z} \to \mathbb{Z}_{p^k} \to \mathbb{Z}_{p^k}/I$. Сквозной гомоморфизм $\mathbb{Z} \to \mathbb{Z}_{p^k}/I$, очевидно является эпиморфизмом и его ядро совпадает с идеалом $(m) \lhd \mathbb{Z}$, поэтому теорема о гомоморфизме дает изоморфизм $\mathbb{Z}_{p^k}/I \cong \mathbb{Z}/(m) = \mathbb{Z}_m = \mathbb{Z}_{p^l}$. Последнее кольцо при $l \geq 2$ содержит нетривиальный нильпотент (образ числа p). Так как факторкольцо по нильрадикалу не содержит нетривиальных нильпотентов получаем, что $\operatorname{Rad} \mathbb{Z}_{p^k} = p\mathbb{Z}_{p^k}$, а фактор по радикалу $\mathbb{Z}_{p^k}/\operatorname{Rad} \mathbb{Z}_{p^k} = \mathbb{Z}_{p^k}/p\mathbb{Z}_{p^k} \cong \mathbb{Z}_p$ является простым полем.

Пусть $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ – произведение степеней попарно различных простых чисел $p_1, \ldots, p_s$. Рассмотрим гомоморфизм $\mathbb{Z} \to \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{k_s}}$, $m \mapsto (\pi_1(m), \ldots, \pi_s(m))$, где $\pi_j : \mathbb{Z} \to \mathbb{Z}_{p_j^{k_j}}$ – канонический эпиморфизм на факторкольцо. По китайской теореме об остатках определенный так гомоморфизм является эпиморфизмом. Его ядро состоит из чисел делящихся одновременно на все $p_j^{k_j}$, а значит, в силу попарной взаимной простоты этих чисел, делящихся на их произведение, т.е. на n. Теорема о гомоморфизме дает изоморфизм $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{k_s}}$. Найдем нильрадикал: $\operatorname{Rad}(\mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{k_s}}) = \operatorname{Rad} \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \operatorname{Rad} \mathbb{Z}_{p_s^{k_s}} = p_1\mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus p_s\mathbb{Z}_{p_s^{k_s}}$. Поскольку p_i обратим в $\mathbb{Z}_{p_j^{k_j}}$ при $i \neq j$, имеем $p_j\mathbb{Z}_{p_j^{k_j}} = p_1 \cdot \ldots \cdot p_s\mathbb{Z}_{p_j^{k_j}}$. Поэтому нильрадикал можно записать как $p_1 \cdot \ldots \cdot p_s \cdot (\mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \operatorname{Rad} \mathbb{Z}_{p_s^{k_s}})$, или как

$\operatorname{Rad}\mathbb{Z}_n = p_1 \cdot \ldots \cdot p_s\mathbb{Z}_n$. Фактор по нильрадикалу $\mathbb{Z}_n/\operatorname{Rad}\mathbb{Z}_n = \mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_s}$ – прямая сумма полей, не содержит нетривиальных нильпотентов.

Приведенные рассуждения показывают, что в $\mathbb{Z}_n$ любой идеал главный, но если n не является простым, то в $\mathbb{Z}_n$ есть делители нуля. Таким образом, $\mathbb{Z}_n$ – кольцо главных идеалов, но не область главных идеалов, если n не является простым.

Пример 4.60. Перечислим все идеалы кольца $\mathbb{Z}_{20}$ и найдем нильрадикал.

Кольцо является абелевой группой по сложению, идеалы являются подгруппами по сложению. Как абелева группа кольцо $\mathbb{Z}_n$ – это циклическая группа, поэтому все ее подгруппы являются циклическими, причем для каждого делителя k порядка n группы есть ровно одна подгруппа порядка k, и порождается она как аддитивная группа классом числа n/k. Если $(m, n) = 1$, то $\langle m\rangle = \mathbb{Z}_n$. Множество таких чисел – это множество $\mathbb{Z}_n^*$ обратимых элементов кольца $\mathbb{Z}_n = \langle m\rangle = (m)$ – подгруппа, порожденная m совпадает с идеалом, порожденным числом m.

Если $(m, 20) = 1$, то $m \in \mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$, $\langle m\rangle = (m) = \mathbb{Z}_{20}$

$\langle 2\rangle = \{2, 4, 6, 810, 12, 14, 16, 18, 0\} = (2)$ – подгруппа, порожденная двойкой, совпадает с идеалом, порожденным числом 2.

$$\begin{aligned}
\langle 4\rangle &= \{4, 8, 12, 16, 0\} = (4)\\
\langle 5\rangle &= \{5, 10, 15, 0\} = (5)\\
\langle 6\rangle &= \{6, 12, 18, 4, 10, 16, 2, 8, 14, 0\} = (6) = (2)\\
\langle 8\rangle &= \{8, 16, 4, 12, 0\} = (8) = (4)\\
\langle 10\rangle &= \{10, 0\} = (10)\\
\langle 12\rangle &= \{12, 4, 16, 8, 0\} = (12) = (4) = (8)\\
\langle 14\rangle &= \{14, 8, 2, 16, 10, 4, 18, 12, 6, 0\} = (14) = (2) = (6)\\
\langle 15\rangle &= \{15, 10, 5, 0\} = (15) = (5)\\
\langle 16\rangle &= \{16, 12, 8, 4, 0\} = (16) = (4) = (8)\\
\langle 18\rangle &= \{18, 16, 14, 12, 10, 8, 6, 4, 2, 0\} = (2)
\end{aligned}$$

Отметим, что $(k) \subset (m) \iff m|k$. Например, $(0) \subset (4) \subset (2) \subset (1) = \mathbb{Z}_{20}$, или $(10) \subset (5)$, $(10) \subset (2)$.

Максимальные идеалы: (2), (5), фактор по ним – поля $\mathbb{Z}_2$ и $\mathbb{Z}_5$ соответственно.

Так как $20 = 2^2 5$, получаем $\operatorname{Rad}\mathbb{Z}_{20} = (10) = 10\mathbb{Z}_{20}$ и $\mathbb{Z}_{20}/(10) \cong \mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5$.

Определение 4.61. Элемент $e \in R$ называется *идемпотентом*, если $e^2 = e$.

Если $e \in R$ – идемпотент, то $1 - e$ – тоже идемпотент. Действительно,

$$(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e.$$

Равенство $e^2 = e$ можно переписать в виде $e(1-e) = 0$, что дает следующее утверждение:

Предложение 4.62. *Элемент $e \in R$ – идемпотент тогда и только тогда, когда $e(1-e) = 0$.*

Теорема 4.63. *Пусть R – ассоциативное, коммутативное кольцо с 1. Оно разложимо в прямую сумму колец в том и только в том случае, когда существует нетривиальный, т.е. отличный от 0 и 1, идемпотент.*

Доказательство. Пусть $R = R_1 \oplus R_2$, тогда единицей кольца служит элемент $(1,1) = (1,0) + (0,1)$. Обозначим $(1,0)$ через e_1, $(0,1)$ – через e_2. Тогда ясно, что $e_1^2 = e_1$, $e_2^2 = e_2$ и $e_2 = 1 - e_1$. Кроме того, $e_1 e_2 = 0$. Ясно также, что e_1, e_2 – нетривиальные идемпотенты.

Пусть в R имеется нетривиальный идемпотент $e = e_1$. Тогда $e_2 = 1 - e = 1 - e_1$ – идемпотент и $e_1 + e_2 = 1$, $e_1 e_2 = 0$. Имеем $r = re_1 + re_2$ для любого $r \in R$, следовательно, $R = Re_1 + Re_2 = (e_1) + (e_2)$. Пересечение этих главных идеалов есть нулевой идеал, так как при умножении на e_2 равенства $r_1 e_1 = r_2 e_2$ получаем $0 = r_2 e_2^2 = r_2 e_2$, а при умножении на e_1 находим, что $r_1 e_1 = 0$. Используя равенства $e_i^2 = e_i$ и $e_1 e_2 = 0$, находим, что $(r_1 e_1 + r_2 e_2)(r_1' e_1 + r_2' e_2) = r_1 r_1' e_1 + r_2 r_2' e_2$. Это означает, что имеет место изоморфизм колец $R \cong R_1 \oplus R_2$, где $R_1 = Re_1$, $R_2 = Re_2$. Единицей в кольце R_i служит e_i, $i = 1, 2$, так как $e_i r_i e_i = r_i e_i e_i = r_i e_i^2 = r_i e_i$. □

Более общо: пусть в кольце R имеются нетривиальные попарно ортогональные идемпотенты e_i, $i = 1, \ldots, s$, т.е. имеются элементы e_i такие, что $e_i^2 = e_i$ и $e_i e_j = 0$ при $i \neq j$. Тогда $R \cong R_1 \oplus \cdots \oplus R_s$, где $R_i = Re_i = (e_i)$.

Обратно, если R изоморфно прямому произведению $R_1 \oplus \cdots \oplus R_s$ колец с единицей, то полагая $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$, где 1 стоит на i-м месте, получаем s нетривиальных попарно ортогональных идемпотентов, сумма которых равна 1.

Идеалы $\mathfrak{a}$, $\mathfrak{b}$ называются *взаимно простыми*, если их сумма равна всему кольцу, т.е. $\mathfrak{a} + \mathfrak{b} = (1)$.

Пользуясь дистрибутивностью, получаем

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b}.$$

Для взаимно простых идеалов отсюда следует включение $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$. С другой стороны, очевидно, что $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. Поэтому

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}, \quad \text{если} \quad \mathfrak{a} + \mathfrak{b} = (1).$$

Пусть A – кольцо (ассоциативное и коммутативное с 1) и $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ – его идеалы. Определим гомоморфизм колец

$$\varphi : A \to \prod_{i=1}^{n} A/\mathfrak{a}_i = \bigoplus_{i=1}^{n} A/\mathfrak{a}_i \quad \text{формулой} \quad \varphi(x) = (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n).$$

Предложение 4.64. (I) *Если* $\mathfrak{a}_i$, $\mathfrak{a}_j$ *взаимно просты при* $i \neq j$, *то* $\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$.

(II) φ *является эпиморфизмом тогда и только тогда, когда идеалы* $\mathfrak{a}_i$, $\mathfrak{a}_j$ *взаимно просты при* $i \neq j$.

(III) φ *является мономорфизмом тогда и только тогда, когда* $\bigcap_{i=1}^{n} \mathfrak{a}_i = (0)$.

Доказательство. (I) доказывается с помощью индукции. Выше было показано, что утверждение верно для $n = 2$. Предположим, что для $n-1$ идеалов результат верен, т.е. $\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i$. Так как $\mathfrak{a}_i + \mathfrak{a}_n = (1)$ при $1 \leq i \leq n-1$, то найдутся $x_i \in \mathfrak{a}_i$, $y_i \in \mathfrak{a}_n$ такие, что $x_i + y_i = 1$, откуда получаем:

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{\mathfrak{a}_\mathrm{n}}.$$

Следовательно, $\mathfrak{b} + \mathfrak{a}_n = (1)$, и поэтому

$$\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

(II) $\Rightarrow$: Покажем, что первые два идеала взаимно просты. Существует $x \in A$ такой, что $\varphi(x) = (1, 0, \ldots, 0)$. Поэтому $1 - x \in \mathfrak{a}_1$ и $x \in \mathfrak{a}_2$, так что

$$1 = (1 - x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2 \;\Rightarrow\; \mathfrak{a}_1 + \mathfrak{a}_2 = (1).$$

Аналогичным образом устанавливается взаимная простота любой другой пары идеалов $\mathfrak{a}_i$, $\mathfrak{a}_j$, $i \neq j$.

$\Leftarrow$: Покажем, что найдется $x \in A$ такой, что $\varphi(x) = (1, 0, \ldots, 0)$. Так как $\mathfrak{a}_1 + \mathfrak{a}_i = (1)$ при $i \neq 1$, найдутся элементы $u_i \in \mathfrak{a}_1$, $v_i \in \mathfrak{a}_i$ такие, что $u_i + v_i = 1$. Положим $x = v_2 \cdot \ldots \cdot v_n$. Тогда $x = (1 - u_2) \cdot \ldots \cdot (1 - u_n) \in 1 + \mathfrak{a}_1$, и $x \in \mathfrak{a}_i$ для $i > 1$, откуда вытекает доказываемое равенство $\varphi(x) = (1, 0, \ldots, 0)$. Аналогичным образом доказывается, что $(0, \ldots, 0, 1, 0, \ldots, 0)$, где 1 стоит на j-м месте, также в образе гомоморфизма φ. Поскольку φ является также гомоморфизмом A-модулей, получаем, что φ – эпиморфизм.

(III) Поскольку $\operatorname{Ker} \varphi = \bigcap_{i=1}^{n} \mathfrak{a}_i$, утверждение очевидно. □

В частности, мы получили утверждение, известное как *китайская теорема об остатках*:

Пусть A – *ассоциативное и коммутативное кольцо с 1 и* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ – *его идеалы такие, что* $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ *при* $i \neq j$ *(т.е. идеалы попарно взаимно просты). Тогда для любых элементов* $x_1, \ldots, x_n \in A$ *найдется* $x \in A$ *такой, что*

$$x \equiv x_i \pmod{\mathfrak{a}_i}, \quad i = 1, \ldots, n$$

.

Из этого предложения и теоремы о гомоморфизме следует, что если идеалы $\mathfrak{a}_i$, $\mathfrak{a}_j$ взаимно просты при $i \neq j$, где $i, j \in \{1, \ldots, n\}$, то имеется изоморфизм

$$A/\prod_{i=1}^{n} \mathfrak{a}_i \cong \prod_{i=1}^{n} A/\mathfrak{a}_i = \bigoplus_{i=1}^{n} A/\mathfrak{a}_i.$$

В частном случае главных и взаимно простых идеалов $\mathfrak{a}_i = (a_i)$, где $a_i \in A$, применяя теорему о гомоморфизме к $\varphi : A \to A/(a_1) \oplus \cdots \oplus A/(a_n)$ получаем:

$$A/(a_1 \cdot \ldots \cdot a_n) \cong A/(a_1) \oplus \cdots \oplus A/(a_n).$$

В частности, мы получаем изоморфизм

$$\mathbb{Z}_{m_1 \cdot \ldots \cdot m_n} \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n},$$

если сомножители попарно взаимно просты, т.е. $(m_i, m_j) = 1$ при $i \neq j$.

Аналогично для многочленов над полем K:

$$K[x]/(f_1 \cdot \ldots \cdot f_n) \cong K[x]/(f_1) \oplus \cdots \oplus K[x]/(f_n),$$

если сомножители $f_i = f_i(x) \in K[x]$ попарно взаимно просты, т.е. $(f_i, f_j) = 1$ при $i \neq j$. Если все многочлены f_i неприводимы, то в правой части стоит сумма полей.

Примеры 4.65. 1. $\mathbb{R}[x]/((x-2)(x-3)(x^2+x+1)) \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{C}$.

Действительно, имеем

$$\mathbb{R}[x]/((x-2)(x-3)(x^2+x+1)) \cong \mathbb{R}[x]/(x-2) \oplus \mathbb{R}[x]/(x-3) \oplus \mathbb{R}[x]/(x^2+x+1).$$

Изоморфизмы $\mathbb{R}[x]/(x-2) \cong \mathbb{R}$, $\mathbb{R}[x]/(x-3) \cong \mathbb{R}$ и $\mathbb{R}[x]/(x^2+x+1) \cong \mathbb{C}$ получаются из теоремы о гомоморфизме: для первых двух рассматриваем гомоморфизмы вычисления $\mathbb{R}[x] \to \mathbb{R}$, определенные соответственно как $f \mapsto f(2)$, $f \mapsto f(3)$, $f \in \mathbb{R}[x]$, а для последнего берем $\mathbb{R}[x] \to \mathbb{C}$, $f \mapsto f(\eta)$, где в качестве η можно взять любой из сопряженных корней уравнения $x^2 + x + 1 = 0$, например, корень $\eta = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Отметим также, что поле разложения многочлена $(x-2)(x-3)(x^2+x+1)$ – это поле $\mathbb{C}$.

2. $\mathbb{Q}[x]/((x-2)(x-3)(x^2+x+1)) \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\eta) = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(i\sqrt{3})$.

Полем разложения многочлена $(x-2)(x-3)(x^2+x+1)$ в данном случае является подполе $Q(\eta) = \mathbb{Q}(i\sqrt{3}) \subset \mathbb{C}$. Его степень расширения над $\mathbb{Q}$ равна двум, поскольку 2 – степень неприводимого над $\mathbb{Q}$ многочлена x^2+x+1. Поле $\mathbb{Q}(\eta) = \mathbb{Q}(i\sqrt{3})$ служит и полем разложения многочлена $x^3 - 1$ над $\mathbb{Q}$, так как $x^3 - 1 = (x-1)(x^2+x+1)$.

4.6 Конечные поля (продолжение)

Сделаем несколько дополнений по поводу расширений конечных полей. Мы знаем, что конечное поле однозначно (с точностью до изоморфизма) определяется числом

$q = p^n$ своих элементов, где p – простое число, равное характеристике поля. Такое конечное поле обозначается через $\mathbb{F}_q = \mathbb{F}_{p^n}$.

Напомним, что на элемент $a \in K$ поля K, имеющего $\operatorname{char} K = p$, гомоморфизм Фробениуса $\Phi : K \to K$, и его степени действуют так: $\Phi(a) = a^p$, $\Phi^2(a) = \Phi(\Phi(a)) = a^{p^2}$, $\Phi^k(a) = a^{p^k}$.

Если $K = \mathbb{F}_{q^m}$, то $\Phi^n(a) = a^{p^n} = a^q$. Положим $\Psi := \Phi^n$. Тогда $\Psi(a) = a^q$. Как мы знаем, любой элемент поля $\mathbb{F}_q$ является корнем многочлена $x^q - x$, поэтому $\Psi|_{\mathbb{F}_q} = \mathrm{id}\,|_{\mathbb{F}_q}$. Аналогично, любой элемент $a \in \mathbb{F}_{q^m}$ является корнем многочлена $x^{q^m} - x$, поэтому $\Psi^m|_{\mathbb{F}_{q^m}} = \mathrm{id}\,|_{\mathbb{F}_{q^m}}$.

Предложение 4.66. *Неприводимый над $\mathbb{F}_q$ многочлен $f \in \mathbb{F}_q[x]$ степени m делит многочлен $x^{q^k} - x$ тогда и только тогда, когда m делит k.*

Доказательство. Пусть $f \mid x^{q^k} - x$, и пусть α – корень многочлена f в его поле разложения над $\mathbb{F}_q$. Тогда $\alpha^{q^k} - \alpha = 0$, откуда следует, что $\alpha \in \mathbb{F}_{q^k}$. Значит простое расщирение $\mathbb{F}_q(\alpha)$ является подполем поля $\mathbb{F}_{q^k}$, и так как $\mathbb{F}_{q^k}$ – векторное пространство над $\mathbb{F}_q(\alpha)$, получаем, что q^k есть степень числа $|\mathbb{F}_q(\alpha)| = q^m$, т.е. m делит k. □

Теорема 4.67. *Пусть $f \in \mathbb{F}_q[x]$ – неприводимый над $\mathbb{F}_q$ многочлен степени m. Тогда $\mathbb{F}_{q^m}$ является его полем разложения, где он имеет m различных простых корней $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$.*

Поля разложения любых многочленов из $\mathbb{F}_q[x]$, неприводимых над $\mathbb{F}_q$ и имеющих одну и ту же степень, изоморфны.

Доказательство. Отметим, что поскольку применение n-й степени гомоморфизма Фробениуса к указанному множеству корней просто переставляет их циклически, можно список корней начать с любого из корней.

Пусть α – произвольный корень многочлена f в его поле разложения над $\mathbb{F}_q$. Тогда степень расширения поля $\mathbb{F}_q(\alpha) = \mathbb{F}_q[x]/(f)$ над $\mathbb{F}_q$ равна m, поэтому $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Поскольку $\Psi = \Phi^n$ – автоморфизм поля $\mathbb{F}_{q^m}$, тождественный на $\mathbb{F}_q$, получаем, что $f(\alpha^{q^k}) = f(\Psi^k(\alpha)) = \Psi^k(f(\alpha)) = \Psi^k(0) = 0$. Следовательно, все перечисленные в теореме элементы являются корнями многочлена f. Покажем, что они различны. Допустим противное. Тогда $\alpha^{q^l} = \alpha^{q^k}$ для некоторых целых чисел l, k таких, что $0 \le l < k \le m - 1$. Возведем это равенство в степень q^{m-k}, и получим равенство

$$\alpha^{q^{m-k+l}} = \alpha^{q^m} = \alpha$$

из которого следует, что α является корнем многочлена $x^{q^{m-k+l}} - x$, поэтому последний делится на f. Но в силу предыдущего предложения это возможно лишь при условии, что $m-k+l$ делится на m. Однако $0 < m-k+l < m$, что приводит к противоречию.

Последнее утверждение следует из установленного в процессе доказательства факта, что полем разложения неприводимого над $\mathbb{F}_q$ многочлена степени m является поле $\mathbb{F}_{q^m}$. □

Поясним, что нужно практически сделать, чтобы явным образом задать изоморфизм между полями разложения двух неприводимых многочленов одинаковой степени.

Пусть K – поле, A – ассоциативная и коммутативная K-алгебра и $a \in A$ – ее элемент. Тогда имеется гомоморфизм вычисления $K[x] \to A$, $f \mapsto f(a)$.

Пусть теперь f, $g \in \mathbb{F}_q[x]$ – неприводимые над полем $\mathbb{F}_q$ многочлены степени m. Поле $L := \mathbb{F}_q[x]/(g)$ является полем разложения как g так и f. Пусть $\theta \in L$ – какой-нибудь корень многочлена f, т.е. $f(\theta) = 0$. Рассмотрим гомоморфизм вычисления

$$\mathbb{F}_q[x] \to L = \mathbb{F}_q[x]/(g), \quad h \mapsto h(\theta), \quad h \in \mathbb{F}_q[x].$$

Легко видеть, что его ядро совпадает с идеалом (f), поэтому возникает гомоморфизм полей

$$\mathbb{F}_q[x]/(f) \to L = \mathbb{F}_q[x]/(g).$$

Поскольку эти поля имеют одну и ту же степень расширения m над полем $\mathbb{F}_q$, построенное отображение – изоморфизм тождественный на $\mathbb{F}_q$.

В частности, если $\alpha, \beta \in \mathbb{F}_q[x]/(f)$ – корни неприводимого над полем $\mathbb{F}_q$ многочлена $f \in \mathbb{F}_q[x]$, то имеется единственный автоморфизм поля $\mathbb{F}_q[x]/(f)$ тождественный на $\mathbb{F}_q$ и переводящий α в β.

Определение 4.68. В расширении $\mathbb{F}_{q^m}$ поля $\mathbb{F}_q$ возьмем произвольный элемент $\alpha \in \mathbb{F}_{q^m}$. Тогда элементы

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$$

называются *сопряженными* с α относительно поля $\mathbb{F}_q$.

Элементы сопряженные с α относительно поля $\mathbb{F}_q$ различны тогда и только тогда, когда минимальный многочлен элемента α над $\mathbb{F}_q$ имеет степень m. Если же степень минимального многочлена элемента α над $\mathbb{F}_q$ меньше m и, скажем, равна d, то d делит m и среди сопряженных с α относительно поля $\mathbb{F}_q$ различными будут только элементы

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}},$$

причем каждый из них повторяется m/d раз в ряду сопряженных.

Определение 4.69. Образующий циклической группы $\mathbb{F}_q^*$ называется *примитивным элементом* поля $\mathbb{F}_q$.

Число примитивных элементов равно $\varphi(q-1)$, где φ – функция Эйлера.

Если $\alpha \in \mathbb{F}_{q^m}$ – примитивный элемент поля $\mathbb{F}_{q^m}$, то $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha] = \mathbb{F}_q(\alpha)$. Действительно, степени примитивного элемента дают все ненулевые элементы поля $\mathbb{F}_{q^m}$.

Минимальный многочлен примитивного элемента поля $\mathbb{F}_{q^m}$ имеет степень m, поскольку $\dim_{\mathbb{F}_q} \mathbb{F}_{q^m} = m$, а так как минимальный многочлен неприводим, получаем, что

Для каждого конечного поля $\mathbb{F}_q$ и любого $m \in \mathbb{N}$ существует многочлен из $\mathbb{F}_q[x]$ неприводимый над $\mathbb{F}_q$ и имеющий степень m.

Теорема 4.70. *В группе $\mathbb{F}_q^*$ элементы, сопряженные с элементом $\alpha \in \mathbb{F}_q^*$ относительно любого подполя поля $\mathbb{F}_q$, имеют один и тот же порядок.*

Доказательство. Мы знаем, что группа $\mathbb{F}_q^*$ – циклическая группа порядка $q-1$. Поскольку степени $p = \operatorname{char}\mathbb{F}_q^*$ взаимно просты с $q-1$, порядки элементов α и α^{p^s} одинаковы. □

Следствие 4.71. *Если α – примитивный элемент поля $\mathbb{F}_q$, то все сопряженные с ним элементы относительно любого подполя поля $\mathbb{F}_q$ также являются примитивными элементами.*

Автоморфизм поля $\mathbb{F}_{q^m}$, тождественный на $\mathbb{F}_q$, называется *автоморфизмом поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$*.

Теорема 4.72. *Любой автоморфизмом поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ совпадает с одним из попарно различных автоморфизмов Ψ^j, $1 \le j \le m$.*

Доказательство. Напомним, что $\Psi^j(a) = a^{q^j}$ для любого $a \in \mathbb{F}_{q^m}$, и $\Psi^m|_{\mathbb{F}_{q^m}} = \mathrm{id}\,|_{\mathbb{F}_{q^m}}$, $\Psi|_{\mathbb{F}_q} = \mathrm{id}\,|_{\mathbb{F}_q}$. Гомоморфизм Ψ^j, очевидно, является мономорфизмом, и, значит, изоморфизмом в силу конечности поля $\mathbb{F}_{q^m}$. Таким образом, Ψ^j – автоморфизм поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$.

С другой стороны, пусть σ – автоморфизм поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$. Пусть β – примитивный элемент поля $\mathbb{F}_{q^m}$ и $m_\beta(x)$ – его минимальный многочлен. Тогда $m_\beta(\sigma(\beta)) = \sigma(m_\beta(\beta)) = \sigma(0) = 0$. Следовательно, $\sigma(\beta)$ – тоже корень минимального многочлена, а поскольку все корни сопряжены, получаем, что $\sigma(\beta) = \beta^{q^j} = \Psi^j(\beta)$ для некоторого j. Поскольку любой ненулевой элемент поля $\mathbb{F}_{q^m}$ является степенью примитивного элемента β, получаем равенство $\sigma(a) = a^{q^j} = \Psi^j(a)$ для любого ненулевого элемента $a \in \mathbb{F}_{q^m}$, что влечет равенство автоморфизмов $\sigma = \Psi^j$. □

Автоморфизмы поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ образуют группу относительно операции композиции автоморфизмов. Очевидно, что эта группа циклическя порядка m с образующим автоморфизмом Ψ.

Пример 4.73. Пусть $\alpha \in \mathbb{F}_{16}$ – корень многочлена $x^4+x+1 \in \mathbb{F}_2[x]$. Сопряженными с ним относительно поля $\mathbb{F}_2$ будут элементы

$$\alpha, \quad \alpha^2, \quad \alpha^4 = \alpha + 1, \quad \alpha^8 = (\alpha^4)^2 = (\alpha+1)^2 = \alpha^2 + 1.$$

Эти элементы являются примитивными элементами поля $\mathbb{F}_{16}$. Сопряженными с α относительно поля $\mathbb{F}_4$ являются только элементы α и $\alpha^4 = \alpha + 1$.

4.7 Делимость в целостных кольцах

Определение 4.74. Пусть A – область целостности и $a, b \in A$. Будем говорить, что a делится на b (пишем $a \vdots b$), или, что b делит a (пишем $b \mid a$), если существует $c \in A$ такой, что $a = cb$.

Делимость, очевидно, можно описать в терминах идеалов так:

$$b \mid a \;\Leftrightarrow\; (a) \subset (b).$$

Определение 4.75. Пусть A – область целостности и $a, b \in A$. Скажем что a ассоциирован с b, и будем писать $a \sim b$, если существует $q \in A^*$ такой, что $a = qb$.

Предложение 4.76. *Ассоциированность является отношением эквивалентности, следовательно, область целостности разбивается на непересекающиеся классы эквивалентности – классы ассоциированных друг с другом элементов.*

Пример 4.77. $\mathbb{Z} = \{0\} \cup \{\pm 1\} \cup \{\pm 2\} \cup \cdots \cup \{\pm n\} \cup \ldots$

Предложение 4.78. *Пусть A – область целостности и $a, b \in A$. Тогда $a \sim b$ в том и только том случае, когда $a \,|\, b$ и $b \,|\, a$.*

Доказательство. Если $a \,|\, b$, то $b = ca$, а из того, что $b \,|\, a$ следует, что $a = db$. Поэтому $a = cda \;\Rightarrow\; cd = 1 \;\Rightarrow\; a \sim b$.

В другую сторону – очевидно. □

Определение 4.79. Пусть A – область целостности и $a, b \in A$. Элемент $d \in A$ называется *общим делителем* элементов a и b, если $d \,|\, b$ и $d \,|\, a$.

Определение 4.80. *Наибольшим общим делителем элементов $a, b \in A$* называется общий делитель элементов a и b, который делится на любой их общий делитель в кольце A.

Наибольший общий делитель обозначают как НОД(a, b) или (a, b).

Определяется очевидным образом и НОД большего числа элементов.

Предложение 4.81. *Если наибольший общий делитель существует, то он единственен с точностью до ассоциированности.*

НОД в целостном кольце может и не существовать, как показывает следующий пример.

Пример 4.82. Пусть $A = \{a_0 + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{R},\ i = 0, 2, 3, \ldots\} \subset \mathbb{R}[x]$ – подкольцо кольца многочленов. Оно является целостным кольцом как подкольцо целостного кольца. Возьмем элементы x^5, $x^6 \in A$ и попробуем найти их общий делитель в A. Многочлены x^5, x^6 имеют разный набор делителей в A и в $\mathbb{R}[x]$. С точностью до обратимых элементов (ими являются нетривиальные многочлены нулевой степени) общие делители многочленов x^5, x^6 таковы:

$1, x, x^2, x^3, x^4, x^5$ в кольце $\mathbb{R}[x]$,

$1, x, x^2, x^3$ в кольце A (так как $x \notin A$, многочлен x^5 не делится в A на x^4, а x^6 не делится на x^5).

Мы видим, что ни один из общих делителей многочленов x^5, x^6 не делится в A на все их общие делители. Следовательно, наибольший общий делитель в A многочленов x^5, x^6 не существует.

Теорема 4.83. *Пусть A – область главных идеалов и $a, b \in A$ – два любых ненулевых элемента. Тогда* НОД(a, b) *существует, причем найдутся $u, v \in A$ такие, что*

$$au + bv = d,$$

где d – наибольший общий делитель элементов a, b.

НОД элементов a и b обозначают (a, b). Равенство $au + bv = d$ в терминах идеалов записывается следующим образом:

$$(d) = (a, b) = (a) + (b),$$

где в правой части стоит главный идеал, порожденный элементом d, а в правой – идеал, порожденный элементами a, b.

Доказательство теоремы. Рассмотрим идеал $(a, b) = (a) + (b)$. Поскольку A – область главных идеалов, существует $d \in A$ такой, что $(a, b) = (d)$. Тогда $a = \xi d$, $b = \eta d$ для подходящих $\xi, \eta \in A$, а это означает, что элемент d является общим делителем элементов a и b. Из равенства $(a, b) = (d)$ также следует, что найдутся $u, v \in A$ такие, что

$$au + bv = d,$$

и из этого равенства видно, что любой общий делитель элементов a и b делит d. □

В частности, НОД есть в кольце целых чисел и в кольце многочленов над полем. Более того, в этих кольцах имеется эффективное средство нахождения НОД – алгоритм Евклида (отсутствующий в общих областях главных идеалов).

Определение 4.84. Ненулевые необратимые элементы области целостности называются *взаимно простыми*, если их наибольшим общим делителем является единица кольца.

Элементы a, b называются *взаимно простыми*, если $(a, b) = 1$, или в терминах идеалов $(a) + (b) = (1)$. Взаимная простота элементов a и b влечет существование таких элементов $u, v \in A$, что $1 = ua + vb$.

Определение 4.85. Ненулевой необратимый элемент области целостности называется *простым элементом*, если его нельзя представить в виде произведения двух необратимых элементов.

Таким образом, элемент является простым, если он делится только на обратимый элемент и на элемент ассоциированный с ним самим.

Пример 4.86. 1. Простые элементы в $\mathbb{Z}$ – это простые числа.

2. Пусть K – поле, тогда $K[x]$ – область главных идеалов, и простой многочлен – это неприводимый многочлен, т.е. многочлен, который нельзя представить в виде произведения двух многочленов положительной степени. В частности, многочлены 1-й степени неприводимы. В случае $\mathbb{C}[x]$ ими неприводимые многочлены исчерпываются. В случае $\mathbb{R}[x]$ неприводимы многочлены первой степени и второй с отрицательным дискриминантом.

Предложение 4.87. *Пусть A – область главных идеалов. Тогда $a \in A$ является простым элементом тогда и только тогда, когда (a) – максимальный идеал кольца A, т.е. $A/(a)$ – поле.*

Доказательство. Пусть a – простой элемент и $b \notin (a)$. Тогда a и b взаимно просты, поэтому существуют такие элементы $u, v \in A$, что $1 = ua + vb$. Но тогда

$$(v + (a))(b + (a)) = 1 + (a),$$

т.е. ненулевой элемент $b+(a) \in A/(a)$ имеет обратный равный $v+(a)$. Следовательно, $A/(a)$ – поле и (a) – максимальный идеал кольца A.

Пусть $A/(a)$ – поле. Покажем, что a – простой элемент. Доказательство проведем от противного. Предположим, что $a = bc$, где b, c – необратимые элементы кольца A. Тогда b не делится на a. Действительно, если предположить, что b делится на a, то $b = sa$ для некоторого $s \in A$, и, следовательно,

$$a = bc = sca \;\Rightarrow\; (sc - 1)a = 0 \;\Rightarrow\; sc = 1 \;\Rightarrow\; c \text{ обратим},$$

и мы получили противоречие. Поэтому b не делится на a, т.е. $b \notin (a)$. Аналогично $c \notin (a)$. Но тогда классы элементов b и c – ненулевые элементы в $A/(a)$, произведение которых равно нулю (т.е. эти классы – делители нуля в $A/(a)$), и мы получили противоречие, поскольку в поле нет делителей нуля. □

Лемма 4.88. *Если простой элемент области главных идеалов делит произведение, то он делит хотя бы один из сомножителей.*

Доказательство. Пусть $p \in A$ – простой элемент, делящий произведение $a_1 \cdot \ldots \cdot a_n$. Обозначим через $\pi : A \to A/(p)$ канонический эпиморфизм на факторкольцо. Если $a_i \notin (p)$ для всех $i = 1, \ldots, n$, то $\pi(a_i) \neq 0$, и, следовательно,

$$\pi(a_1 \cdot \ldots \cdot a_n) = \pi(a_1) \cdot \ldots \cdot \pi(a_n) \neq 0,$$

поскольку $A/(p)$ – поле. Но тогда $a_1 \cdot \ldots \cdot a_n \notin (p)$. □

Докажем аналог основной теоремы арифметики для области главных идеалов.

Теорема 4.89. *Любой ненулевой необратимый элемент области главных идеалов может быть разложен в конечное произведение простых элементов, причем это разложение единственно с точностью до порядка и ассоциированности.*

Доказательство от противного. Пусть не все элементы могут быть разложены, назовем их плохими. Пусть a_0 плохой, то есть ненулевой необратимый, и его нельзя разложить. Простые элементы не являются плохими, так как они сами являются разложением на простые множители. Поэтому a_0 не является простым, и, значит, $a_0 = a_1 b_1$ – произведение двух необратимых ненулевых элементов, причем хотя бы один из них плохой. Пусть a_1 плохой, тогда имеем строгое вложение $(a_0) \subset (a_1)$. Далее поступаем с a_1 аналогичным образом, т.е. зная, что этот элемент не является простым представляем его в виде произведения двух необратимых ненулевых элементов и берем тот сомножитель a_2, который является плохим. Получаем строгое вложение $(a_1) \subset (a_2)$. Продолжая так дальше, получаем бесконечную цепочку строго возрастающих идеалов

$$(a_0) \subset (a_1) \subset \cdots \subset (a_n) \subset \ldots$$

Обозначим объединение этих идеалов через I. Докажем, что это идеал. Непустота очевидна. Сумма двух элементов лежит. Противоположный лежит. Умножение на любой элемент выдерживает. Поскольку в A каждый идеал является главным, I порожден некоторым элементом a, т.е. $I = (a)$. Но этот элемент обязан принадлежать некоторому (a_i), а тогда $(a) = I \subset (a_i) \subset I$, т.е. $I = (a_i)$, поэтому цепочка стабилизируется – противоречие. Итак, плохих элементов нет, то есть все элементы раскладываются в произведение простых элементов.

Остается доказать единственность. Если a простой, то он не может быть представлен как произведение нескольких простых, т.е. разложение единственно. Если $a = p_1 \dots p_n = q_1 \dots q_m$, то p_1 делит правую часть, значит (по лемме) делит один из q_i. Пусть делит q_1, тогда $q_1 = sp_1$, и в силу простоты элемента q_1 элемент s обратим. Сокращаем на p_1 и т.д. (т.е. завершаем доказательство индукцией по n). □

Определение 4.90. Ассоциативное и коммутативное кольцо с единицей называют *нётеровым*, если любая возрастающая цепочка идеалов стабилизируется, т.е. если имеется возрастающая цепочка идеалов

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots \subset \mathfrak{a}_n \subset \dots,$$

то начиная с некоторого m все идеалы одинаковы: $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \dots$.

В доказательстве предыдущей теоремы был получен следующий результат.

Теорема 4.91. *Область главных идеалов является нётеровым кольцом.*

Вернемся к рассмотрению простых элементов.

Определение 4.92. Целостное кольцо с однозначным (в смысле ассоциированности) разложением на простые множители называется *факториальным кольцом.*

Таким образом, факториальное кольцо – это область целостности, в которой справедлив аналог основной теоремы арифметики. По доказанному, область главных идеалов является факториальным кольцом.

Следствие 4.93. *Любой элемент a области главных идеалов A может быть разложен в произведение простых множителей:*

$$a = sp_1^{m_1} \cdot \dots \cdot p_l^{m_l},$$

где $s \in A^*$ обратим, а все p_i – различные простые элементы кольца A. Если b делит a, то

$$b = tp_1^{k_1} \cdot \dots \cdot p_l^{k_l},$$

где $t \in A^*$ обратим и $0 \le k_i \le m_i$, $i = 1, \dots, l$.

НОД двух элементов в области главных идеалов ищется очевидным образом с помощью разложения элементов на простые множители. Определено также *наименьшее общее кратное* (НОК) нескольких элементов и его можно найти с помощью разложения этих элементов в произведение простых сомножителей.

Примеры 4.94.

1. $\mathbb{Z}$ – факториальное кольцо.

2. Кольцо многочленов над полем является факториальным кольцом. Простые элементы – неприводимые многочлены.

3. Кольцо многочленов над факториальным кольцом является факториальным кольцом. Поэтому и кольцо многочленов от n переменных над факториальным кольцом является факториальным кольцом.

4. Кольцо $A = \mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3} \mid a, b \in \mathbb{Z}\}$ не является факториальным кольцом, и, следовательно, не является областью главных идеалов. Утверждение следует из того, что некоторые элементы этого кольца можно по разному разложить в произведение простых элементов. А именно,

$$4 = 2 \cdot 2, \qquad 4 = (1 + i\sqrt{3})(1 - i\sqrt{3}).$$

Мы покажем, что 2 и $1 \pm i\sqrt{3}$ – простые элементы кольца A, и поэтому в A нет однозначного разложения на простые множители.

Определим функцию

$$N : A \to \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$$

формулой

$$N(z) := |z|^2 = |a + ib\sqrt{3}|^2 = a^2 + 3b^2.$$

Ясно, что $N(z_1 z_2) = N(z_1)N(z_2)$, поэтому элемент z обратим в том и только в том случае, когда $N(z) = 1 \;\Rightarrow\; z = \pm 1$. Таким образом, $A^* = \{\pm 1\}$.

Покажем, что 2 – простой элемент. Предположим противное, тогда $2 = z_1 z_2$, где сомножители необратимы, и, следовательно,

$$N(z_k) > 1 \text{ для } k = 1, 2 \;\Rightarrow\; N(z_k) \geq 2^2 = N(2).$$

Поскольку $N(2) = N(z_1)N(z_2)$, получаем противоречие.

Поскольку $N(1 \pm i\sqrt{3}) = |1 \pm i\sqrt{3}|^2 = 4$, аналогичное рассуждение доказывает простоту элементов $1 \pm i\sqrt{3}$.

Наконец, отметим, что 2 и $1 \pm i\sqrt{3}$, очевидно, не являются ассоциированными, поэтому мы имеем два разных представления элемента 4 в произведение простых элементов.

4.8 Евклидовы кольца

Определение 4.95. *Евклидовым кольцом* называется область целостности A с заданной на ней функцией (нормой) $N : A \setminus \{0\} \to \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$ такой, что

1) $N(ab) \geq N(a)$.

2) Для любых a и b, где $b \neq 0$, существуют q и r такие, что $a = qb + r$, причем или $r = 0$, или $N(r) < N(b)$.

Отметим, что если b необратим, то a не делится на ab. Разделив a на ab с остатком, получим:

$$a = q(ab) + r \;\Rightarrow\; r = a(1 - qb) \;\Rightarrow\; N(a) \leq N(r) < N(ab).$$

Если же b обратим, то с одной стороны $N(ab) \geq N(a)$, а с другой

$$a = (ab)b^{-1} \;\Rightarrow\; N(a) = N((ab)b^{-1}) \geq N(ab),$$

и, следовательно, $N(ab) = N(a)$. Таким образом, неравенство $N(ab) \geq N(a)$ превращается в равенство тогда и только тогда, когда элемент b обратим.

Отметим также, что при делении с остатком единственности неполного частного и остатка не требуется.

Теорема 4.96. *Евклидово кольцо является областью главных идеалов.*

Доказательство. Если I – ненулевой идеал, то возьмем $b \in I$ такой, что

$$N(b) = \min_{x \in I \setminus \{0\}} N(x).$$

Докажем, что $I = (b)$. Если это не так, в I найдется элемент a, который не делится на b. Поэтому существуют q и $r \neq 0$ такие, что

$$a = qb + r, \quad \text{где} \;\; N(r) < N(b) \;\Rightarrow\; r = a - qb \in I \;\; \text{и} \; N(r) < N(b) = \min_{x \in I \setminus \{0\}} N(x) \leq N(r)$$

– противоречие. □

Поскольку область главных идеалов является факториальным кольцом, получаем, что евклидово кольцо факториально.

НОД можно найти в евклидовом кольце с помощью алгоритма Евклида.

Пусть $N(a) \geq N(b)$. Используя деление с остатком получим:

$$\begin{aligned}
&a = q_1 b + r_1, \quad N(r_1) < N(b);\\
&b = q_2 r_1 + r_2, \quad N(r_2) < N(r_1);\\
&r_1 = q_3 r_2 + r_3, \quad N(r_3) < N(r_2);\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{k-2} = q_k r_{k-1} + r_k, \quad N(r_k) < N(r_{k-1});\\
&r_{k-1} = q_{k+1} r_k.
\end{aligned}$$

Элемент r_k является НОД элементов a и b. Действительно, рассматривая последовательно равенства снизу вверх убеждаемся в том, что r_k делит a и b. С другой стороны, двигаясь сверху вниз, мы видим, что если s делит a и b, то он делит r_1, далее из второго равенства получается, что s делит r_2, и т.д. Из предпоследнего равенства получается, что s делит r_k.

Ясно, что $\mathbb{Z}$ – евклидово кольцо. В качестве нормы целого числа берется его модуль: $N(m) := |m|$.

Кольцо многочленов $K[x]$ над полем K – евклидово кольцо с нормой

$$N(f) := \deg f, \quad 0 \neq f \in K[x].$$

Еще один важный пример евклидова кольца – это кольцо целых гауссовых чисел.

Пример 4.97. *Целые гауссовы числа.* Это – подкольцо $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ своего поля частных $\mathbb{Q}(i) \subset \mathbb{C}$. Определим норму формулой

$$N(z) = N(a + ib) = a^2 + b^2 = |z|^2.$$

Тогда $N(z) \geq 1$, где z – любое ненулевое целое гауссово число, и $N(z_1 z_2) = N(z_1)N(z_2)$. Обратимые элементы этого кольца должны иметь норму равную 1. Поэтому $(\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$. Деление с остатком производится следующим образом. Пусть $z = z_1/z_2 \in \mathbb{C}$, где z_1, z_2 – целые гауссовы числа, $z_2 \neq 0$. В общем случае z не является гауссовым числом. Но если в качестве q взять ближайшее к z гауссово число, то $|z - q| \leq 1/\sqrt{2}$, откуда получаем, что $z_1 = qz_2 + r$, где $r = z_1 - qz_2$, и

$$N(r) = |z_1 - qz_2|^2 = |z_2|^2|z - q|^2 \leq \frac{|z_2|^2}{2} < |z_2|^2 = N(z_2) \;\Rightarrow\; N(r) < N(z_2).$$

Тот факт, что ближайшее к заданному комплексному числу целое гауссово число находится на расстоянии не большем, чем $1/\sqrt{2}$, видно из геометрических соображений. Целые гауссовы числа – вершины квадратной сетки, а в квадрате со стороной 1 наиболее удаленной точкой от вершин является центр квадрата, расстояние от которого до вершин равно половине длины диагонали квадрата, т.е. равно $\sqrt{2}/2 = 1/\sqrt{2}$.

Итак, $\mathbb{Z}[i]$ является евклидовым кольцом, следовательно, является областью главных идеалов, а, значит, и факториальным кольцом.

Число 3 является простым элементом, а 2 – нет, поскольку

$$2 = (1 + i)(1 - i) = -i(1 + i)^2 = i(1 - i)^2,$$

и $1 \pm i$ – простые элементы.

Еще один пример разложения на простые (одинаковые разложения с точностью до ассоциированности):

$$5 = (2 + i)(2 - i) = (-2 - i)(-2 + i) = (1 - 2i)(1 + 2i).$$

Здесь $2 \pm i$ – простые элементы, и, как можно проверить, $2 + i$ и $2 - i$ не являются ассоциированными.

В китайской теореме об остатках для евклидовых колец можно сделать следующее небольшое дополнение.

Пусть A – евклидово кольцо и $a_1, \ldots, a_n$ – его попарно взаимно простые элементы. Тогда для любых элементов $x_1, \ldots, x_n \in A$ найдется $x \in A$ такой, что

$$x \equiv x_i \,(\mathrm{mod}\ a_i), \quad i = 1, \ldots, n,$$

причем любые два решения этой системы сравнений сравнимы по модулю элемента $a_1 \cdot \ldots \cdot a_n$ (т.е. их разность делится на $a_1 \cdot \ldots \cdot a_n$), и существует единственное решение x, что $N(x) < N(a_1 \cdot \ldots \cdot a_n)$.

Например, если $A = K[x]$ – кольцо многочленов над полем K, и рассматривается система сравнений

$$f \equiv g_i \,(\mathrm{mod}\ f_i), \quad i = 1, \ldots, n,$$

где $f_1, \ldots, f_n$ попарно взаимно просты и $g_1, \ldots, g_n$ – произвольно заданные многочлены. Тогда имеется единственный многочлен f степени $\deg f < \deg f_1 \cdot \ldots \cdot f_n$, являющийся решением указанной системы сравнений.

Если внимательно посмотреть на доказательство существования и единственности разложения элементов области главных идеалов в произведение простых элементов, то обнаруживается, что для существования разложения достаточно предположить нётеровость кольца, а для доказательства единственности разложения нужно чтобы целостное кольцо обладало следующим свойством: из делимости произведения двух элементов на простой элемент следует, что хотя бы один из сомножителей делится на этот простой элемент, а это эквивалентно требованию простоты главного идеала, порожденного произвольным простым элементом. Таким образом, имеют место следующие две теоремы, доказательства которых повторяют части доказательства факториальности области главных идеалов.

Теорема 4.98. *Предположим, что в целостном кольце главный идеал порожденный любым простым элементом прост. Тогда если элемент этого кольца разложен в произведение простых элементов, то это разложение единственно с точностью до перестановки сомножителей и ассоциированности.*

Доказательство. Покажем сначала, что если при сделанных предположениях простой элемент делит произведение некоторых элементов кольца, то он делит хотя бы один из сомножителей. Пусть $p \in A$ – простой элемент, делящий $a_1 \cdot \ldots \cdot a_n$. Обозначим через $\pi : A \to A/(p)$ канонический эпиморфизм на факторкольцо, являющееся целостным кольцом, поскольку идеал (p) прост. Если $a_i \notin (p)$ для всех $i = 1, \ldots, n$, то $\pi(a_i) \neq 0$, и, следовательно,

$$\pi(a_1 \cdot \ldots \cdot a_n) = \pi(a_1) \cdot \ldots \cdot \pi(a_n) \neq 0,$$

поскольку $A/(p)$ – область целостности. Но тогда $a_1 \cdot \ldots \cdot a_n \notin (p)$, и полученное противоречие доказывает сделанное утверждение.

Если a представлен ввиде произведения простых элементов двумя способами

$$a = p_1 \ldots p_n = q_1 \ldots q_m,$$

то p_1 делит правую часть, а, значит, делит один из q_i. После перенумерации простых элементов в правой части можно считать, что p_1 делит q_1, тогда $q_1 = sp_1$, и в силу простоты элемента q_1 элемент s обратим. Сокращаем на p_1 и т.д. (т.е. завершаем доказательство индукцией по n). □

Теорема 4.99. *В нётеровом кольце любой ненулевой необратимый элемент может быть разложен в произведение простых элементов.*

Доказательство от противного. Напомним, что ассоциативное и коммутативное кольцо с единицей называется нётеровым, если любая возрастающая цепочка идеалов стабилизируется.

Пусть не все элементы могут быть разложены, назовем их плохими. Пусть a_0 плохой, то есть ненулевой необратимый, и его нельзя разложить. Простые

элементы не являются плохими, так как они сами являются разложением на простые множители. Поэтому a_0 не является простым, и, значит, $a_0 = a_1 b_1$ – произведение двух необратимых ненулевых элементов, причем хотя бы один из них плохой. Пусть a_1 плохой, тогда имеем строгое вложение $(a_0) \subset (a_1)$. Далее поступаем с a_1 аналогичным образом, т.е. зная, что этот элемент не является простым, представляем его в виде произведения двух необратимых ненулевых элементов и берем тот сомножитель a_2, который является плохим. Получаем строгое вложение $(a_1) \subset (a_2)$. Продолжая так дальше, получаем бесконечную цепочку строго возрастающих идеалов

$$(a_0) \subset (a_1) \subset \cdots \subset (a_n) \subset \ldots$$

Обозначим объединение этих идеалов через I. Докажем, что это идеал. Непустота очевидна. Сумма двух элементов лежит. Противоположный лежит. Умножение на любой элемент выдерживает. Поскольку кольцо A нётерово, цепочка стабилизируется – противоречие. Итак, плохих элементов нет, то есть все элементы раскладываются в произведение простых элементов. □

4.9 Нётеровы кольца

Можно дать следующее определение нётерова кольца.

Определение 4.100. Ассоциативное и коммутативное кольцо с единицей называют *нётеровым*, если выполняется любое из эквивалентных условий:

1) всякий идеал конечно порожден,
2) не существует бесконечной строгой возрастающей цепочки идеалов.

Покажем, что условия действительно эквивалентны.

Если имеется строго возрастающая цепочка идеалов

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \ldots,$$

то идеал $\mathfrak{b} := \bigcup\limits_{i=1}^{\infty} \mathfrak{a}_i$ равный объединению всех идеалов не является конечно порожденным. Действительно, если предположить, что он порожден элементами $x_1, \ldots, x_k$, т.е. $\mathfrak{b} = (x_1, \ldots, x_k)$, то поскольку $x_i \in \mathfrak{a}_{m_i}$ при некотором m_i, все эти элементы $x_1, \ldots, x_k$ лежат в $\mathfrak{a}_s$, где $s = \max\limits_i(m_i)$. Но тогда $\mathfrak{b} \subset \mathfrak{a}_s \subset \mathfrak{b}$. Поэтому $\mathfrak{b} = \mathfrak{a}_s$, что означает стабилизацию цепочки идеалов: $\mathfrak{a}_s = \mathfrak{a}_{s+1} = \ldots$.

Если есть не конечно порожденный идеал, то в кольце можно найти такие элементы x_i, $i \in \mathbb{N}$, что $x_{i+1} \notin \mathfrak{a}_i := (x_1, \ldots, x_i)$. Тем самым имеется строго возрастающая цепочка идеалов $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \ldots$.

Мы знаем, что область главных идеалов является нётеровым кольцом. В частности, кольца $\mathbb{Z}$ и $K[x]$, где K – поле, нётеровы.

Предложение 4.101. *Факторкольцо нётерова кольца является нётеровым.*

Доказательство. Возьмем прообраз идеала при каноническом эпиморфизме на факторкольцо. Это будет конечно порожденный идеал. Образы его образующих в факторкольце дают образующие идеала факторкольца. □

Из теоремы о гомоморфизме для колец следует, что гомоморфный образ нётерова кольца является нётеровым кольцом.

Предложение 4.102. *В нётеровом кольце любой идеал содержит некоторую степень своего радикала.*

Доказательство. Напомним, что радикал $r(I)$ идеала $I \subset A$ – это идеал кольца A, состоящий из элементов $a \in A$ таких, что $a^n \in I$ для некоторого $n = n(a) \in \mathbb{N}$. Можно сказать по-другому: радикал идеала I – прообраз нильрадикала факторкольца A/I при каноническом эпиморфизме $A \to A/I$.

Пусть $r(I) = (x_1, \ldots, x_k)$. Имеем $x_i^{n_i} \in I$, $i = 1, \ldots, k$. Идеал $r(I)^N$ порождается элементами $x_1^{s_1} \cdot \ldots \cdot x_k^{s_k}$, где $\sum\limits_{i=1}^{k} s_i = N$. Положим $N = k \cdot \max\limits_{1 \le i \le k} n_i$. Тогда для некоторого j имеем $s_j \ge n_j \;\Rightarrow\; x^{s_j} \in I \;\Rightarrow\; x_1^{s_1} \cdot \ldots \cdot x_k^{s_k} \in I$. Таким образом, все элементы, порождающие идеал $r(I)^N$, лежат в I, а, значит, $r(I)^N \subset I$. □

Из этого предложения, взяв в качестве идеала нётерова кольца нулевой идеал получаем:

Следствие 4.103. *В нётеровом кольце нильрадикал нильпотентен.*

Иными словами: в нётеровом кольце некоторая степень нильрадикала равна нулевому идеалу.

Перейдем к рассмотрению модулей над нётеровым кольцом.

Лемма 4.104. *1. Фактормодуль конечнопорожденного модуля конечно порожден.*

2. Если подмодуль и фактормодуль по этому подмодулю конечно порождены, то и сам модуль конечно порожден.

Доказательство. Первое утверждение очевидно – фактормодуль порождается образами образующих модуля.

Пусть A-модули M' и $M'' = M/M'$ конечно порождены. Покажем, что M конечно порожден. Пусть

$$M' = \langle x_1, \ldots, x_k \rangle = \{a_1 x_1 + \cdots + a_k x_k \mid a_1, \ldots, a_k \in A\}$$

и $M'' = \langle \alpha_1, \ldots, \alpha_m \rangle$, $\alpha_i = y_i + M'$, $y_i \in M$. Тогда

$$M = \langle x_1, \ldots, x_k, y_1, \ldots, y_m \rangle.$$

Действительно, возьмем произвольный элемент $z \in M$ и рассмотрим его образ $\pi(z)$ в фактормодуле M'' при гомоморфизме факторизации $\pi : M \to M'' = M/M'$. Имеются элементы кольца $b_1, \ldots, b_m \in A$ такие, что $\pi(z) = b_1\alpha_1 + \cdots + b_m\alpha_m$. Положим $\widetilde{z} = b_1 y_1 + \cdots + b_m y_m$. Тогда

$$\pi(\widetilde{z}) = b_1\pi(y_1) + \cdots + b_m\pi(y_m) = b_1\alpha_1 + \cdots + b_m\alpha_m = \pi(z) \;\Rightarrow\; \pi(z - \widetilde{z}) = 0 \;\Rightarrow\; z - \widetilde{z} \in M'.$$

Найдутся $a_1, \ldots, a_k \in A$ такие, что

$$z - \widetilde{z} = a_1 x_1 + \cdots + a_k x_k \;\Rightarrow\; z = a_1 x_1 + \cdots + a_k x_k + b_1 y_1 + \cdots + b_m y_m$$

□

Теорема 4.105. *Всякий подмодуль конечно порожденного модуля над нётеровым кольцом конечно порожден.*

Доказательство. Проведем доказательство индукцией по числу порождающих. Пусть модуль порождается всего одним элементом. Такой модуль называют *циклическим*. Если рассматривать A как модуль над собой, то циклические подмодули в A – это в точности главные идеалы (рассматриваемые как A-модули).

Циклический модуль изоморфен факторкольцу A/I по некоторому идеалу I. Факторкольцо в данном случае рассматривается как A-модуль. Действительно, если $M = \langle x \rangle$, то отображение $A \to M$, $a \mapsto ax$, как легко проверить, является эпиморфизмом A-модулей. Поэтому из теоремы о гомоморфизме для модулей получаем изоморфизм $M \cong A/I$, где I – ядро указанного эпиморфизма. Пусть M' – подмодуль модуля M. Его прообраз в A – это идеал J, содежащий I. В силу нётеровости кольца A идеал J порождается конечным числом элементов и, значит, образы этих элементов в M' порождают M'. Впрочем, указанный факт следует из первого утверждения леммы.

Предположим, что утверждение верно для модулей с числом порождающих не превосходящем $n-1$. Докажем для M с числом порождающих равным n. Итак, пусть $M' \subset M = \langle x_1, \ldots, x_n \rangle$. Положим $L := \langle x_1, \ldots, x_{n-1} \rangle$ и $L' := M' \cap L$. Тогда L' – подмодуль в L и, значит, конечно порожден в силу индуктивного предположения. С другой стороны, L' – подмодуль в M', а фактормодуль M'/L' изоморфен подмодулю модуля M/L. Действительно, рассмотрим образ подмодуля M' при каноническом гомоморфизме $M \to M/L$. По теореме о гомоморфизме образ изоморфен фактормодулю модуля M' по ядру гомоморфизма, а ядро, очевидно, есть L'. Модуль M/L является циклическим, поскольку порожден образом элемента x_n, и, по уже доказанному, любой его подмодуль конечно порожден. Итак, L' и M/L' конечно порождены и из второго утверждения леммы получаем, что M' конечно порожден. □

Теорема 4.106 (Теорема Гильберта о базисе идеала)**.** *Пусть A – нётерово кольцо. Тогда кольцо многочленов $A[x]$ над кольцом A является нётеровым кольцом.*

Доказательство. Пусть $I \lhd A[x]$. Положим $I_n := I \cap P_n$, где

$$P_n = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid a_0, \ldots, a_n \in A\}.$$

P_n является свободным A-модулем с базисом $\{1, x, x^2, \ldots, x^n\}$. Следовательно, его подмодуль I_n конечно порожден над A. Ясно также, что $I_n \subset I_{n+1}$. Нам же нужно показать, что конечно порожденным над $A[x]$ является идеал $I = \bigcup\limits_{i=0}^{\infty} I_n$. Обозначим через J_n множество коэффициентов при x^n всех многочленов из I_n вместе с нулем. Тогда J_n – идеал кольца A. Поскольку I – идеал кольца $A[x]$, имеем $xI \subset I \Rightarrow J_n \subset J_{n+1}$. Таким образом, имеем возрастающую цепочку идеалов кольца A, которая в силу нётеровости кольца A обязана стабилизироваться. Пусть $J_m = J_{m+1} = \ldots$. Для многочлена $f \in I_n$ степени n, где $n > m$, найдем многочлен $g \in I_m$ степени m с таким же старшим коэффициентом, что и у многочлена f. Тогда $f - x^{n-m} g \in I_{n-1}$. Если степень полученного многочлена все еще больше

m, скажем равна $l > m$ (т.е. $f - x^{n-m}g \in I_l$), то найдем $h \in I_m$ с подходящим старшим коэффициентом так, чтобы $f - x^{n-m}g - x^{l-m}h \in I_{l-1}$. Ясно, что продолжая действовать таким же образом дальше, мы в результате получим многочлен из I_m. Следовательно, $f \in A[x] \cdot I_m \;\Rightarrow\; I \subset A[x] \cdot I_m \subset I \;\Rightarrow\; I = A[x] \cdot I_m$. Поскольку I_m конечно порожден над A, найдутся порождающие его над A многочлены $g_1, \ldots, g_s$, и эти же многочлены будут порождающими элементами для I над кольцом $A[x]$.

□

Следствие 4.107. *Для любого $n \in \mathbb{N}$ кольцо многочленов от n переменных над нётеровым кольцом нётерово.*

Доказательство. Можно применить индукцию, поскольку $A[x_1, \ldots, x_n] \cong R[x_n]$, где $R = A[x_1, \ldots, x_{n-1}]$. □

Следствие 4.108. *Кольцо, конечно порожденное над нётеровым подкольцом, нётерово.*

Доказательство. Пусть A – подкольцо кольца R такое, что $R = A[r_1, \ldots, r_n]$. Последнее равенство означает, что любой элемент кольца R записывается в виде многочлена от элементов $r_1, \ldots, r_n$ с коэффициентами из A. Можно сказать по другому: гомоморфизм вычисления $A[x_1, \ldots, x_n] \to R$, ставящий в соответетствие многочлену $f = f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ элемент $f(r_1, \ldots, r_n) \in R$, является эпиморфизмом. Таким образом, R является факторкольцом кольца многочленов над кольцом A по некоторому идеалу. Если A нётерово, то кольцо многочленов над кольцом A тоже нётерово и нётеровым является факторкольцо, которое изоморфно R по теореме о гомоморфизме.

□

На прошлой лекции было доказано, что любой подмодуль конечно порожденного над нётеровым кольцом модуля конечно порожден над этим кольцом.

Предложение 4.109. *Пусть $A \subset B \subset C$ – кольца (ассоциативные, коммутативные и с общей единицей) и A нётерово. Предположим, что C конечно порождено как A-алгебра и конечно порождено как B-модуль. Тогда B конечно порождено как A-алгебра.*

Доказательство. Пусть $c_1, \ldots, c_m$ порождают C как A-алгебру и $y_1, \ldots, y_n$ порождают C как B-модуль. Существуют $b_{ij}, d_{ijk} \in B$ такие, что

$$c_i = \sum_j b_{ij} y_j,$$
$$y_i y_j = \sum_k d_{ijk} y_k.$$

Обозначим через B_0 алгебру, порожденную над A элементами $b_{ij}, d_{ijk} \in B$. Таким образом, $A \subset B_0 \subset B$. Поскольку кольцо, конечно порожденное над нётеровым подкольцом, нётерово, мы видим, что B_0 нётерова.

Поскольку $C = A[c_1, \ldots, c_n]$, мы видим, что в силу приведенных выше представлений элементов c_i, $y_i y_j$, любой элемент из является линейной комбинацией элементов $y_1, \ldots, y_n$ с коэффициентами из B_0. Это означает, что C – конечно порожденный B_0-модуль. Таким образом, B – подмодуль конечнопорожденного модуля над нётеровым кольцом, а значит он тоже конечно порожден, т.е. B – конечно порожденный B_0-модуль. И так как кольцо B_0 конечно порождено как A-алгебра, то и кольцо B конечно порождено как A-алгебра. □

Предложение 4.110. *Пусть K – поле и L – конечно порожденная K-алгебра. Тогда если L тоже является полем, то L – конечное алгебраическое расширение поля K.*

Доказательство. Проведем доказательство от противного, т.е. предположим, что L не алгебраично над K. Тогда можно считать, что $L = K[a_1, \ldots, a_n]$, где $a_1, \ldots, a_r$ ($r \geq 1$) алгебраически независимы, а остальные элементы $a_{r+1}, \ldots, a_n$ алгебраичны над полем $F := K(a_1, \ldots, a_r)$. Тогда L будет конечным алгебраическим расширением поля F, и, следовательно, будет конечномерным векторным пространством над F. Применив предыдущее предложение к тройке $K \subset F \subset L$, видим, что F – конечно порожденная K-алгебра. Следовательно, $F = K[y_1, \ldots, y_s]$ для некоторых $y_1, \ldots, y_s \in F$. Каждый из элементов y_j имеет вид $y_j = f_j/g_j$, где f_j, g_j – многочлены от $a_1, \ldots, a_r$. В кольце $K[a_1, \ldots, a_r]$ имеется бесконечно много неприводимых многочленов, поэтому существует неприводимый многочлен h взаимно простой со всеми многочленами g_j (например, можно взять неприводимый делитель многочлена $1 + g_1 \cdot \ldots \cdot g_s$). Тогда обратный элемент $h^{-1} \in F$ не может быть многочленом от y_j, и мы получили противоречие. Следовательно, L – алгебраическое расширение поля K конечной степени. □

Следствие 4.111. *Пусть K – поле, A – конечно порожденная K-алгебра и $\mathfrak{m}$ – ее максимальный идеал. Тогда поле $A/\mathfrak{m}$ – конечное алгебраическое расширение поля K. В частности, если K алгебраически замкнуто, то $A/\mathfrak{m} \cong K$.*

Доказательство. Сделанное утверждение прямо следует из предыдущего предложения, если положить $L = A/\mathfrak{m}$. □

4.10 Алгебраические множества

Пусть K – поле, $\mathbb{A}^n = \mathbb{A}^n_K := K^n$ будем называть n-мерным аффиным пространством.

Определение 4.112. *Алгебраическое подмножество* в $\mathbb{A}^n$ (замкнутое алгебраическое аффинное подмногообразие) – это множество совместных нулей какой-либо совокупности многочленов от n-переменных.

Ясно, что множество совместных нулей совокупности многочленов от n-переменных совпадает с множеством совместных нулей многочленов из идеала, порожденного многочленами из выбранной совокупности многочленов. Из теоремы Гильберта о базисе следует, что кольцо $K[x_1, \ldots, x_n]$ нётерово, поэтому любой его идеал конечно порожден. Отсюда следует, что любое алгебраическое подмножество является

множеством совместных нулей конечного набора многочленов. Если обозначить через $V(f) \subset \mathbb{A}^n$ множество нулей многочлена $f \in K[x_1, \ldots, x_n]$, а через $V(f_1, \ldots, f_k)$ – множество совместных нулей многочленов $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$, то

$$V(f_1, \ldots, f_k) = V(f_1) \cap \cdots \cap V(f_k).$$

Пусть $J \subset K[x_1, \ldots, x_n]$ – идеал. Обозначим через $V(J) \subset \mathbb{A}^n$ множество совместных нулей всех многочленов из J. Ясно, что $V((f)) = V(f)$, где (f) – главный идеал, порожденный многочленом f, и

$$V(J) = \bigcap_{f \in J} V(f).$$

Пусть $X \subset \mathbb{A}^n$. Обозначим через $I(X) \subset K[x_1, \ldots, x_n]$ идеал, состоящий из всех многочленов обращающихся в ноль во всех точках подмножества X. Если X – алгебраическое множество, то $V(I(X)) = X$. Действительно, если X – множество совместных нулей некоторых многочленов $f_1, \ldots, f_k$, т.е.

$$X = V(f_1, \ldots, f_k) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n \mid f_i(a_1, \ldots, a_n) = 0,\ i = 1, \ldots, n\},$$

то $f_1, \ldots, f_k \in I(X)$, поэтому множество совместных нулей многочленов $f_1, \ldots, f_k$ совпадает с множеством совместных нулей многочленов из $I(X)$, и это дает равенство $V(I(X)) = X$.

С другой стороны, рассмотрим $I(V(J))$. Из определений ясно, что этот идеал содержит идеал J, т.е. $J \subset I(V(J))$. Если $f^m \in J$, то поскольку $V(f) = V(f^m)$, получаем, что $f \in I(V(J))$. Следовательно, радикал идеала J содержтся в $I(V(J))$:

$$\sqrt{J} = r(J) \subset I(V(J)).$$

Сопоставление

$$\{\text{идеалы кольца } K[x_1, \ldots, x_n]\} \xrightarrow{V} \{\text{алгебраические множества}\}, \quad J \mapsto V(J),$$

обладает следующими свойствами:

(I) $V(0) = \mathbb{A}^n$, $V(1) = \varnothing$,
(II) $J_1 \subset J_2 \ \Rightarrow\ V(J_2) \subset V(J_1)$,
(III) $V(J_1 \cap J_2) = V(J_1) \cup V(J_2)$,
(IV) $V(\sum\limits_{\alpha \in B} J_\alpha) = \bigcap\limits_{\alpha \in B} V(J_\alpha)$.

Доказательства требует только третье свойство, остальные очевидны, при этом ясно, что $V(J_1 \cap J_2) \supset V(J_1) \cup V(J_2)$. Таким образом, остается только установить обратное включение $V(J_1 \cap J_2) \subset V(J_1) \cup V(J_2)$. Доказательство проведем от противного. Если $(a_1, \ldots, a_n) \notin V(J_1) \cup V(J_2)$, то найдутся многочлены f_i, $i = 1, 2$, такие, что $f_i(a_1, \ldots, a_n) \neq 0$, $i = 1, 2$. Но тогда $(a_1, \ldots, a_n) \notin V(f_1 \cdot f_2)$, и поэтому $(a_1, \ldots, a_n) \notin V(J_1 \cap J_2)$.

Отображение

$$\{\textbf{подмножества в } \mathbb{A}^n\} \xrightarrow{I} \{\textbf{идеалы кольца } K[x_1, \ldots, x_n]\}, \quad X \mapsto I(X),$$

как было показано выше, обладает следующими свойствами:

(I) $X_1 \subset X_2 \Rightarrow I(X_1) \supset I(X_2)$,

(II) $X \subset V(I(X))$, причем $X = V(I(X)) \Leftrightarrow X$ является алгебраическим множеством,

(III) Для любого идеала $J \in K[x_1, \ldots, x_n]$ имеем $\sqrt{J} \subset I(V(J))$.

Предложение 4.113. *Предположим, что поле K алгебраически замкнуто. Тогда любой максимальный идеал кольца многочленов $K[x_1, \ldots, x_n]$ имеет вид*

$$\mathfrak{m}_P = (x_1 - a_1, \ldots, x_n - a_n),$$

где $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ – некоторая точка, т.е. совпадает с идеалом $I(P) := I(\{P\})$ всех функций, обращающихся в ноль в точке P.

Доказательство. Пусть $\mathfrak{m} \subset K[x_1, \ldots, x_n]$ – максимальный идеал. Тогда

$$L := K[x_1, \ldots, x_n]/\mathfrak{m}$$

– конечно порожденная K-алгебра и одновременно поле, поскольку $\mathfrak{m}$ – максимальный идеал. В силу того, что поле K алгебраически замкнуто из следствия 4.111 вытекает, что $L \cong K$. Пусть $\varphi : K \to L$ – композиция вложения $K \subset K[x_1, \ldots, x_n]$ и канонического гомоморфизма на фактор $\pi : K \to L = K[x_1, \ldots, x_n]/\mathfrak{m}$. Поскольку φ – изоморфизм, у него есть обратный и мы можем положить $a_i := \varphi^{-1}(\pi(x_i))$. Тогда $x_i - a_i \in \operatorname{Ker} \pi = \mathfrak{m}$, $i = 1, \ldots, n$. Следовательно, идеал $(x_1 - a_1, \ldots, x_n - a_n)$ содержится в $\mathfrak{m}$. С другой стороны, идеал $(x_1 - a_1, \ldots, x_n - a_n)$ максимален и поэтому $(x_1 - a_1, \ldots, x_n - a_n) = \mathfrak{m}$. □

Теорема 4.114 (Теорема Гильберта о нулях)**.** *Предположим, что поле K алгебраически замкнуто. Тогда*

(I) Пусть $J \subset K[x_1, \ldots, x_n]$ – собственный идеал, тогда $V(J) \neq \varnothing$.

(II) $I(V(J)) = \sqrt{J}$ для любого идеала $J \subset K[x_1, \ldots, x_n]$.

Доказательство. $J \subset K[x_1, \ldots, x_n]$ – собственный идеал. Тогда он содержится в некотором максимальном идеале

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n).$$

Но тогда $(a_1, \ldots, a_n) \in V(f)$ для любого $f \in J$, и поэтому $(a_1, \ldots, a_n) \in V(J)$. Следовательно, $V(J) \neq \varnothing$.

Второе утверждение выводится из первого следующим образом. Пусть $J \subset K[x_1, \ldots, x_n]$ – произвольный идеал и $f \in K[x_1, \ldots, x_n]$. Добавим еще одну переменную z и рассмотрим новый идеал

$$J_1 := (J, tf - 1) \subset K[x_1, \ldots, x_n, t],$$

порожденный идеалом J и многочленом $tf - 1$. Тогда

$$Q = (a_1, \ldots, a_n, b) \in V(J_1) \subset \mathbb{A}^{n+1}$$

в том и только том случае, когда

$$g(P) = g(a_1, \ldots, a_n) = 0 \ \ \forall g \in J \Leftrightarrow P = (a_1, \ldots, a_n) \in V(J)$$

и

$$bf(P) = 1, \text{ т.е. } f(P) \neq 0 \text{ и } b = f(P)^{-1}.$$

Рассмотрим $f \in K[x_1, \ldots, x_n]$ такой, что $f(P) = 0$ для всех $P \in V(J)$. Тогда $V(J_1) = \varnothing$ и из уже доказанного первого утверждения теоремы следует, что $J_1 = (1)$. Поэтому найдутся $f_i \in J$ и $g_0, g_i \in K[x_1, \ldots, x_n, t]$ такие, что

$$1 = \sum_i g_i f_i + g_0(tf - 1) \in K[x_1, \ldots, x_n, t].$$

Пусть t^N – наибольшая из степеней переменной t, входящих в g_0 и все g_i. Если умножить соотношение на f^N, то получим

$$f^N = \sum_i G_i(x_1, \ldots, x_n, tf) f_i + G_0(x_1, \ldots, x_n, tf)(tf - 1),$$

где многочлен $G_i = f^N g_i$ записан как многочлен от переменных $x_1, \ldots, x_n$ и tf. Так как $t^s f^s = 1 + t^s f^s - 1 = 1 + (tf - 1)(...)$, мы можем переписать правую часть так, что получим соотношение в кольце многочленов $K[x_1, \ldots, x_n, t]$

$$f^N = \sum_i h_i(x_1, \ldots, x_n) f_i + h_0(x_1, \ldots, x_n, t)(tf - 1).$$

Поскольку левая часть и сумма в правой части не зависят от t, последнее слагаемое, содержащее множитель $tf - 1$, тождественно равно нулю. Следовательно,

$$f^N = \sum_i h_i f_i \in J,$$

так как $f_i \in J$. □

Из теоремы Гильберта о нулях следует, что определенные выше отображения I и V определяют взаимнообратные биекции

$$\{\textbf{радикальные идеалы}\} \leftrightarrow \{\textbf{алгебраические подмножества}\}.$$

Действительно, $X = V(I(X))$ для любого алгебраического множества, а для любого радикального идеала J теорема Гильберта дает $I(V(J)) = \sqrt{J} = J$ (напомним, что идеал J называется радикальным, если $J = \sqrt{J}$).

Замечание 4.115. Без предположения алгебраической замкнутости поля теорема Гильберта о нулях перестает быть верной. Например, рассмотрим в кольце $\mathbb{R}[x_1, x_2]$ главный идеал J, порожденный многочленом $x_1^2 + x_2^2 + 1$. Ясно, что этот идеал не совпадает со всем кольцом и $V(J) = \varnothing$.

Определение 4.116. Алгебраическое множество называется *неприводимым*, если его нельзя представить в виде объединения двух непустых алгебраических множеств $X = X_1 \cup X_2$ таких, что $X_i \neq X$, $i = 1, 2$.

Предложение 4.117. *Пусть $X \subset \mathbb{A}^n$ – алгебраическое множество и $I(X)$ – соответствующий ему идеал. Тогда X неприводимо тогда и только тогда, когда идеал $I(X)$ является простым.*

Любое алгебраическое множество является конечным объединением неприводимых компонент, т.е. имеет представление

$$X = X_1 \cup \cdots \cup X_s,$$

где алгебраические множества X_i неприводимы и $X_i \not\subset X_j$ для $i \neq j$.

Доказательство. Покажем сначала, что алгебраическое множество X приводимо тогда и только тогда, когда идеал $I(X)$ не является простым. Пусть $X = X_1 \cup X_2$ и X_1, X_2 – собственные алгебраические подмножества множества X, т.е. подмножества не совпадающие с X и с пустым множеством. Тогда найдутся $f_i \in I(X_i) \setminus I(X)$, $i = 1, 2$. Произведение $f_1 f_2$ обращается в ноль на всех точках множества X, поэтому $f_1 f_2 \in I(X)$, и следовательно, идеал $I(X)$ не является простым.

Обратно. Если $I(X)$ не прост, то существуют $f_1, f_2 \notin I(X)$ такие, что $f_1 f_2 \in I(X)$. Положим $I_i := (I(X), f_i)$, $X_i := V(I_i)$, $i = 1, 2$. Тогда X_i строго содержится в X, $i = 1, 2$ и значит, $X_1 \cup X_2 \subset X$. С другой стороны, если произведение двух многочленов обращается в ноль в некоторой точке, то в этой точке обращается в ноль хотя бы один из многочленов, поэтому $X \subset X_1 \cup X_2$. Тем самым доказано, что $X = X_1 \cup X_2$.

Перейдем к доказательству второго утверждения. Покажем, что убывающие цепочки алгебраических подмножеств в $\mathbb{A}^n$ стабилизируются, т.е. для любой такой цепочки

$$X_1 \supset X_2 \supset \cdots \supset X_n \supset \ldots$$

найдется номер N такой, что $X_N = X_{N+1} = \ldots$. Этот факт сразу следует из стабилизации (в силу нётеровости кольца многочленов) возрастающей цепочки идеалов

$$I(X_1) \subset I(X_2) \subset \cdots \subset I(X_n) \subset \ldots.$$

Будем доказывать от противного. Алгебраическое множество, которое нельзя разложить на неприводимые будем называть плохим. Плохое множество приводимо (поскольку неприводимое множество не является плохим). Следовательно, оно представляется как объединение двух собственных алгебраических множеств, и хотя бы одно из них плохое. Это плохое множество приводимо и в его представлении в объединение двух собственных подмножеств снова есть плохое подмножество. Продолжая так дальше мы получаем, убывающую цепочку плохих алгебраических множеств. Но цепочка стабилизируется и мы получаем противоречие – с одной стороны мы получили неприводимое множество, а с другой оно является плохим. □

Простой идеал является радикальным. Из теоремы Гильберта о нулях следует, что определенные выше отображения I и V определяют взаимнообратные биекции

$$\{\textbf{простые идеалы}\} \leftrightarrow \{\textbf{неприводимые алгебраические подмножества}\}.$$

4.11 Конечно порожденные модули над областью главных идеалов

Пусть M – модуль над ассоциативным и коммутативным кольцом с единицей R и I – идеал кольца R. Тогда множество конечных сумм элементов модуля M вида im, $i \in I$, $m \in M$, является подмодулем модуля M. Этот подмодуль обозначают как IM. Ясно, что M/IM является таким R-модулем, что при умножении любого его элемента на произвольный элемент идеала I всегда получается ноль. Поэтому на M/IM корректно определена структура модуля над факторкольцом R/I.

Напомним, что свободный модуль ранга n – это R-модуль $R \oplus \cdots \oplus R$ – прямая сумма n модулей изоморфных R. Такой модуль принято обозначать как R^n. Удобно также считать, что свободный модуль нулевого ранга – это нулевой модуль.

Ранг свободного модуля определен однозначно, т.е. свободные модули изоморфны в том и только том случае, когда они имеют равные ранги. Действительно, возьмем в R какой-нибудь максимальный идеал $\mathfrak{m}$. Тогда $K := M/\mathfrak{m}$ – поле и

$$(R \oplus \cdots \oplus R)/(\mathfrak{m}R \oplus \cdots \oplus \mathfrak{m}R) = R/\mathfrak{m} \oplus \cdots \oplus R/\mathfrak{m} = K \oplus \cdots \oplus K$$

– векторное пространство над K. Поскольку размерность векторного пространства однозначно определена (любые два базиса имеют одинаковое число элементов), получаем требуемое. Отметим также, что при выборе другого максимального идеала получается другое поле, но размерность над ним возникающего векторного пространства та же самая.

Предложение 4.118. *Всякий подмодуль конечно порожденного свободного модуля над областью главных идеалов тоже свободен и конечно порожден и его ранг не превосходит ранга содержащего его свободного модуля.*

Доказательство. Проведм индукцию по рангу свободного модуля. Если ранг равен единице, то имеем подмодуль свободного модуля ранга 1, т.е. имеем идеал области главных идеалов. Если этот идеал нетривиален, то он равен (a), где $a \in R$ – ненулевой элемент кольца R. Но (a) и R изоморфны как R-модули. Действительно, модульный гомоморфизм $R \to (a)$, $r \mapsto ra$, очевидно, является эпиморфизмом, и является мономорфизмом в силу того, что в R нет делителей нуля. Таким образом, подмодуль является свободным модулем ранга 1, а его базис состоит из единственного элемента a.

Предположим, что утверждение верно для подмодулей свободных модулей ранга не превосходящего $n-1$. Пусть M – свободный модуль ранга n и N – его подмодуль. Запишем M в виде $M = R \oplus M'$, где M' – свободный модуль ранга $n-1$, и рассмотрим факторизацию по первому слагаемому $\pi : R \oplus M' \to M'$. Положим $N' := \pi(N)$. По предположению индукции N' свободен и его ранг не превосходит

$n-1$. Возьмем какой-нибудь базис в N' и рассмотрим в $N \subset M$ его прообраз. Это будет набор линейно независимых элементов в M (поскольку образ при π нетривиальной линейной комбинации этих элементов есть нетривиальная линейная комбинация базисных элементов модуля N'). Построенный набор элементов порождает подмодуль $\widetilde{N} \subset N \subset M$, изоморфно отображающийся на N' при гомоморфизме π. Его ранг не превосходит $n-1$. Ясно, что первое слагаемое R в прямой сумме $M = R \oplus M'$ есть ядро отображения π, т.е. $R = \operatorname{Ker}\pi$. Положим $N'' = N \cap \operatorname{Ker}\pi = N \cap R$. Тогда $N'' \cap \widetilde{N} = \{0\}$ и $N'' + \widetilde{N} = N$, т.е. $N'' \oplus \widetilde{N} = N$. Модуль N'' тоже свободен как подмодуль свободного модуля ранга 1. Поэтому N – прямая сумма двух свободных модулей, сумма рангов которых не превосходит n. Таким образом, N свободен и его ранг не превосходит n. □

Теорема 4.119 (Об инвариантных множителях)**.** *Пусть R – область главных идеалов и M – свободный R-модуль ранга n. Тогда для любого подмодуля $N \subset M$ в M существует базис $e_1, \ldots, e_n$ и существуют ненулевые элементы $\lambda_1, \ldots, \lambda_m \in R$, $m \leq n$, что*

1) $\lambda_1 e_1, \ldots, \lambda_m e_m$ является базисом N,

2) $\lambda_i | \lambda_{i+1}$, $i = 1, \ldots, m-1$.

С точностью до умножения на обратимые элементы кольца набор множителей $\lambda_1, \ldots, \lambda_m$ не зависит от выбора такого базиса.

Напомним, что циклический модуль – это модуль порождаемый одним элементом. Если M – такой модуль и m – порождающий его элемент, то гомоморфизм R-модулей $R \to M$, $r \mapsto rm$, является эпиморфизмом и по теореме о гомоморфизме $M \cong R/I$, где I – ядро построенного эпиморфизма. Если R – область главных идеалов, то циклический модуль изоморфен $R/(a)$, где (a) – главный идеал в R, порожденный некоторым элементом $a \in R$.

Следствие 4.120. *Конечно порожденный модуль над областью главных идеалов изоморфен прямой сумме циклических модулей.*

Доказательство. Пусть R – область главных идеалов и M – конечно порожденный R-модуль. Пусть $m_1, \ldots, m_n$ – порождающие элементы. Тогда гомоморфизм

$$R^n \to M, \quad (r_1, \ldots, r_n) \mapsto r_1 m_1 + \cdots + r_n m_n,$$

очевидно, является эпиморфизмом. Его ядро N – свободный модуль ранга не превосходящего n и $M \cong R^n/N$. По теореме 4.129 можно найти такой базис модуля R^n, что

$$N = (\lambda_1) \oplus \cdots \oplus (\lambda_m) \subset R^m \oplus R^{n-m} \;\Rightarrow\; M \cong R/(\lambda_1) \oplus \cdots \oplus R/(\lambda_m) \oplus R^{n-m}.$$

□

Если $\lambda = p^k$, где p – простой элемент область главных идеалов R и $k \in \mathbb{N}$, то циклический модуль

$$R/(\lambda) = R/(p^k)$$

называют *примарным циклическим модулем.*

В случае $R = \mathbb{Z}$ примарный циклический модуль – это примарная абелева группа $\mathbb{Z}_{p^k}$, p – простое число.

Если $\lambda = up_1^{k_1} \cdots p_s^{k_s}$, где $p_1, \ldots, p_s$ – различные простые элементы и $u \in R^*$, то

$$R/(\lambda) \cong R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_s^{k_s}),$$

поэтому справедливо следующее утверждение:

Следствие 4.121. *Конечно порожденный модуль над областью главных идеалов изоморфен прямой сумме свободного модуля и примарных циклических модулей.*

В частном случае $R = \mathbb{Z}$ получаем:

Теорема 4.122. *Всякая конечно порожденная абелева группа изоморфна прямой сумме бесконечных циклических и примарных циклических групп. Число бесконечных циклических групп и порядки примарных циклических групп определены однозначно.*

Следствие 4.123. *Всякая конечная абелева группа изоморфна прямой сумме примарных циклических групп, причем набор порядков этих примарных циклических групп определен однозначно.*

Следствие 4.124. *Всякая конечно порожденная абелева группа не имеющая элементов конечного порядка (кроме нуля) свободна.*

Основная теорема выводится из следующего предложения.

Предложение 4.125. *Для любой матрицы $C \in M_{m\times k}(R)$ с элементами из области главных идеалов R существуют такие обратимые матрицы $F \in GL(m, R)$ и $G \in GL(k, R)$, что матрица $D = FCG$ является диагональной, причем $\lambda_i := d_{ii}|\lambda_j$ при $i < j$. Матрица D зависит только от C и не зависит от выбора матриц F, G.*

Предложение 4.126. *Пусть $\varphi : R \to S$ – гомоморфизм колец и M – S-модуль. Положим $rm = \varphi(r)m$, где $r \in R$, $m \in M$. Тогда введенное умножение превращает M в R-модуль.*

Эту конструкцию называют отступлением вдоль гомоморфизма.

Задача 4.127. Показать, что отступление вдоль гомоморфизма дает ковариантный функтор из категории S-модулей в категорию R-модулей.

Пусть A – линейный оператор, действующий в n-мерном векторном пространстве V над полем K. Обозначим через $L(V) = \mathrm{End}_K(V)$ алгебру линейных операторов на V. Ясно, что V является $L(V)$-модулем. Для любого многочлена $f(t) \in K[t]$ определен оператор $f(A)$, и отображение вычисления

$$K[t] \to L(V), \quad f \mapsto f(A),$$

является гомоморфизмом K-алгебр. Отсюда следует, что на V можно смотреть как на $K[t]$-модуль. Умножение вектора $v \in V$ на многочлен $f(t)$ есть применение оператора $f(A)$ к вектору v:

$$f(t) \cdot v = f(A)v.$$

Таким образом, действие оператора A на V соответствует умножению на t. В данном случае в разложении отсутствует свободная часть, поскольку свободный $K[t]$-модуль (положительного ранга) бесконечномерен над K.

Пусть K – алгебраически замкнутое поле. Тогда примарные циклические модули имеют вид:

$$K[t]/((t-\alpha)^m), \quad \alpha \in K.$$

Пусть $\pi : K[t] \to K[t]/((t-\alpha)^m)$ канонический эпиморфизм на фактормодуль. В базисе

$$\{\pi((t-\alpha)^{m-1}), \ldots, \pi(t-\alpha), \pi(1) = 1\}$$

оператор умножения на t записывается жордановой клеткой $J(\alpha)$. В жордановой клетке главная диагональ состоит из одинаковых элементов равных α, а диагональ, расположенная выше на одну позицию состоит из единиц. Все остальные элементы жордановой клетки – нули.

Матрица, состоящая из жордановых клеток (расположенных по главной диагонали) называется жордановой матрицей.

Теорема 4.128. *Всякий линейный оператор в конечномерном пространстве над алгебраически замкнутым полем в некотором базисе записывается жордановой матрицей, которая определена однозначно с точностью до перестановки клеток.*

Теорема 4.129 (Об инвариантных множителях)**.** *Пусть R – область главных идеалов и M – свободный R-модуль ранга n. Тогда для любого подмодуля $N \subset M$ в M существует базис $e_1, \ldots, e_n$ и существуют ненулевые элементы $\lambda_1, \ldots, \lambda_m \in R$, $m \leq n$, что*

1) $\lambda_1 e_1, \ldots, \lambda_m e_m$ является базисом N,

2) $\lambda_i | \lambda_{i+1}$, $i = 1, \ldots, m-1$.

С точностью до умножения на обратимые элементы кольца набор множителей $\lambda_1, \ldots, \lambda_m$ не зависит от выбора такого базиса.

Основная теорема выводится из следующего предложения.

Предложение 4.130. *Для любой матрицы $C \in M_{n\times k}(R)$ с элементами из области главных идеалов R существуют такие обратимые матрицы $F \in GL(n,R)$ и $G \in GL(k,R)$, что матрица $D = FCG$ является диагональной, причем $\lambda_i := d_{ii}|\lambda_j$ при $i < j$. Матрица D зависит только от C и не зависит от выбора матриц F, G.*

Доказательство теоремы 4.129. Пусть $T = \{f_1, \dots, f_n\}$ – какой-нибудь базис модуля M и $U = \{u_1, \dots, u_k\}$ – любой порождающий подмодуль N набор его элементов. Обозначим чере $C \in M_{n\times k}(R)$ матрицу перехода от базиса T к набору элементов U. Это значит, что мы разлагаем элементы u_i по базису T и координаты записываем в столбцы. Тогда

$$U = T \cdot C, \quad \text{или более подробно:} \quad (u_1 \dots u_k) = (f_1 \dots f_n) \cdot C.$$

Применим предложение 4.130 к матрице C: существуют невырожденные матрицы $F \in GL(n,R)$ и $G \in GL(k,R)$, что $D = FCG$ является диагональной, т.е. $D = (d_{ij})$, $d_{ij} = 0$ $i \neq j$, и $\lambda_i|\lambda_j$, при $i < j$, где $\lambda_i = d_{ii}$.

$$U = T \cdot C \;\Leftrightarrow\; U = TF^{-1}FCGG^{-1} = TF^{-1}DG^{-1} \;\Leftrightarrow\; UG = TF^{-1}D.$$

Последнее соотношение перепишем в виде

$$(v_1 \dots v_k) = (e_1 \dots e_n)D, \quad \text{где} \quad (e_1 \dots e_n) = TF^{-1}, \;\; (v_1 \dots v_k) = UG.$$

Поскольку матрицы F и G обратимы, $E = \{e_1, \dots, e_n\}$ – базис модуля M, а $V = \{v_1, \dots, v_k\}$ – набор порождающих подмодуль N элементов. Если $\lambda_i = d_{ii} \neq 0$ при $i \leq m \leq k$, и $d_{ii} = 0$ при $i > m$, то подмодуль N порождается элементами $\{\lambda_1 e_1, \dots, \lambda_m e_m\}$, которые линейно независимы, и, следовательно, образуют базис подмодуля N. □

Доказательство предложения 4.130. Элементарными преобразованиями над строками назовем преобразования вида:

1. прибавление к одной строке другой строки умноженный на произвольный элемент кольца,

2. перестановка строк,

3. умножение строки на обратимый элемент кольца.

Аналогичные элементарные преобразования имеются и для столбцов.

Хорошо известно, что элементарные преобразования над строками (столбцами) можно реализовать посредством умножения справа и слева на обратимые матрицы. Можно с помощью матриц с определителем 1 делать *обобщенные элементарные преобразования*, состоящие в том, что две выделенные строки (два столбца) заменяются на их линейные комбинации, а остальные строки (столбцы) не изменяются.

Пусть $(a,b) = d$ и $a = a_1 d$, $b = b_1 d$, $(a_1, b_1) = 1$. Тогда найдутся элементы кольца x, y такие, что $a_1 x + b_1 y = 1$, $xa + yb = d$.

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} x & -b_1 \\ y & a_1 \end{pmatrix} = \begin{pmatrix} d & 0 \end{pmatrix}, \quad \begin{pmatrix} x & y \\ -b_1 & a_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}, \quad \begin{vmatrix} x & -b_1 \\ y & a_1 \end{vmatrix} = \begin{vmatrix} x & y \\ -b_1 & a_1 \end{vmatrix} = 1.$$

С помощью элементарных и обобщенных элементарных преобразований любую матрицу можно привести к диагональному виду. При этом преобразования задаются умножениями слева и справа на обратимые матрицы. □

5 Представления групп

Пусть V – векторное пространство над полем K и $\dim_K V = n$. Через $GL(V)$ и $L(V)$ обозначались группа обратимых операторов и алгебра всех операторов на пространстве V соответственно. При выборе базиса $GL(V)$ отождествляется с группой невырожденных матриц $GL(n, K)$, а $L(V)$ – с алгеброй всех матриц $M_{n\times n}(K)$.

Определение 5.1. *Пусть G группа, K поле и V – векторное пространство над полем K размерности n. Любой гомоморфизм $\varphi : G \to GL(V)$ называется линейным представлением группы G в векторном пространстве V или n-мерным представлением группы G над полем K.*
Если $K = \mathbb{C}$ – поле комплексных чисел, то представление называется комплексным.
Если ядро гомоморфизма φ тривиально, то представление называется точным.

Таким образом, если φ – линейное представление группы G, то

$$\varphi(gh) = \varphi(g)\varphi(h) \quad \text{и} \quad \varphi(e) = \mathrm{id}_V,$$

где $\varphi(g)\varphi(h) = \varphi(g) \circ \varphi(h)$ – композиция операторов. При выборе базиса в V операторы записываются матрицами и тогда $\varphi(g)\varphi(h)$ – произведение матриц.

Определение 5.2. *Пусть A – K-алгебра, где K – поле. Гомоморфизм алгебр $T : A \to L(V)$ называется линейным представлением алгебры A в векторном пространстве V или n-мерным представлением алгебры A. Если ядро гомоморфизма T тривиально, то представление называется точным.*

Таким образом, если T – гомоморфизм, то

$$T(a + b) = T(a) + T(b), \quad T(ab) = T(a)T(b), \quad T(\lambda a) = \lambda T(a),\ a, b \in A,\ \lambda \in K.$$

Пример 5.3. Напомним, что с конечной группой G связана алгебра – групповая алгебра группы G:

$$K[G] = \left\{ \sum_{g\in G} a_g g \mid g \in G,\ a_g \in K \right\},$$

в которой сложение и умножение элементов производится по формулам

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g, \quad \left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h gh.$$

Ясно, что представление конечной группы дает представление ее групповой алгебры и наоборот представление групповой алгебры определяет представление группы.

На линейные представления группы можно смотреть с разных позиций и использовать несколько терминологий.

1. Линейное представление группы G – это гомоморфизм $\varphi : G \to GL(V)$ в группу обратимых линейных операторов векторного пространства V над полем K.

2. Если выбрать какой-нибудь базис в V, то при $\dim_K V = n$ получается матричное представление – гомоморфизм в группу невырожденных матриц $G \to GL(n, K)$.

3. Представление – это линейное действие $G \times V \to V$, $(g, v) \mapsto gv = \varphi(g)v$. Морфизмы линейных представлений – линейные эквивариантные отображения.

4. Линейное представление группы G – это $K[G]$-модуль V (G-модуль для краткости), где $K[G]$ – групповая алгебра группы G.

Часто, говоря о представлении, удобно просто указывать пространство представления V, подразумевая наличие линейного действия на нем группы.

Определение 5.4. *Пусть $\varphi : G \to GL(V)$ – представление и $U \subset V$ – подпространство. Тогда подпространство U называется инвариантным относительно представления φ, если оно инвариантно для каждого оператора $\varphi(g)$, т.е. $\varphi(g)(U) \subset U$ для любого $g \in G$.*

Таким образом, инвариантное относительно представления φ подпространство U определяет представление $\psi : G \to GL(U)$, которое называют *подпредставлением* представления φ.

Если есть представления $\varphi_i : G \to GL(V_i)$, $i = 1, \ldots, m$, то очевидным образом определяется их *прямая сумма* $\varphi = \varphi_1 \oplus \ldots \oplus \varphi_m$:

$$\varphi : G \to GL(V), \quad V = V_1 \oplus \ldots \oplus V_m, \quad \varphi(g)((v_1, \ldots, v_m)) := (\varphi_1(g)(v_1), \ldots, \varphi_m(g)(v_m)).$$

Определение 5.5. Представление называется *приводимым*, если у него есть нетривиальное инвариантное подпространство (подпространство не совпадающее со всем пространством и нулевым подпространством). Представление, у которого нет нетривиальных инвариантных подпространств называется *неприводимым*. Представление называется *вполне приводимым*, если оно раскладывается в прямую сумму неприводимых представлений.

Одномерные представления, очевидно, являются неприводимыми.

Инвариантные подпространства, приводимые, неприводимые и вполне приводимые представления для алгебр определяются аналогичным образом.

Определение 5.6. Пусть $\varphi : G \to GL(V)$ и $\psi : G \to GL(W)$ – линейные представления. Морфизмом представления φ в представление ψ называется такое линейное отображение $\Phi : V \to W$, что для любого $g \in G$

$$\Phi \circ \varphi(g) = \psi(g) \circ \Phi : V \to W.$$

Таким образом, для любых $v \in V$ и $g \in G$ имеют место равенства

$$\Phi(\varphi(g)(v)) = \psi(g)(\Phi(v)).$$

С помощью представлений φ и ψ мы можем определить действия группы G на V и W соответственно:

$$(g, v) \mapsto \varphi(g)(v), \ v \in V; \qquad (g, w) \mapsto \psi(g)(w), \ w \in W.$$

Тогда видно, что морфизм представлений φ в ψ – это просто линейное эквивариантное отображение G-пространства V в G-пространство W. Таким образом, представления образуют подкатегорию в категории G-пространств и эквивариантных отображений.

В случае когда $\Phi : V \to W$ – изоморфизм векторных пространств представления φ и ψ называются *эквивалентными* (*изоморфными, подобными*). Эквивалентность представлений, как легко проверить, является отношением эквивалентности.

Таким образом, на линейные представления группы можно смотреть с разных позиций и использовать несколько терминологий.

1. Линейное представление группы G – это гомоморфизм $\varphi : G \to GL(V)$ в группу обратимых линейных операторов векторного пространства V над полем K.

2. Если выбрать какой-нибудь базис в V, то при $\dim_K V = n$ получается матричное представление – гомоморфизм в группу невырожденных матриц $G \to GL(n, K)$.

3. Представление – это линейное действие $G \times V \to V$, $(g, v) \mapsto gv = \varphi(g)v$. Морфизмы линейных представлений – линейные эквивариантные отображения.

4. Линейное представление группы G – это $K[G]$-модуль V (G-модуль для краткости), где $K[G]$ – групповая алгебра группы G.

Часто, говоря о представлении, удобно просто указывать пространство представления V, подразумевая наличие линейного действия на нем группы.

Теорема 5.7. *Морфизм неприводимых представлений либо является изоморфизмом, либо нулевым отображением.*

Доказательство. Утверждение следует из того, что если $\Phi : V \to W$ – морфизм представления $\varphi : G \to GL(V)$ в $\psi : G \to GL(W)$, то $\operatorname{Ker}\Phi$ – инвариантное подпространство в V, а $\operatorname{Im}\Phi$ – инвариантное подпространство в W. □

Теорема 5.8 (лемма Шура)**.** *Пусть $\Phi : V \to V$ – эндоморфизм неприводимого представления $\varphi : G \to GL(V)$ и поле K алгебраически замкнуто. Тогда эндоморфизм $\Phi : V \to V$ скалярен.*

Доказательство. Обозначим через $\mathcal{E} : G \to GL(V)$ представление группы G такое, что любой элемент $g \in G$ переходит при гомоморфизме $\mathcal{E}$ в тождественный оператор $\mathcal{E}(g) = \mathrm{id}_V$. Поскольку эндоморфизм Φ перестановочен с любым $\varphi(g)$, эндоморфизм $\Phi - \lambda\mathcal{E}$ при любом λ тоже перестановочен с любым $\varphi(g)$. Поскольку поле алгебраически замкнуто, у Φ есть собственный вектор с некоторым собственным значением γ. Но тогда по предыдущей теореме $\Phi - \gamma\mathcal{E} = 0$, т.е. Φ скалярен. □

Следствие 5.9. *Пусть $\varphi : G \to GL(V)$ $\psi : G \to GL(W)$ – два неприводимых представления группы G в пространствах V и W над алгебраически замкнутым полем. Тогда любые два морфизма представления φ в представление ψ пропорциональны.*

Доказательство. Очевидно, что утверждение верно в случае когда один из морфизмов равен нулю. Если оба морфизма ненулевые, то они – изоморфизмы. Обозначим эти изоморфизмы через $\Phi, \Psi : V \to W$. Тогда $\Psi^{-1} \circ \Phi : V \to V$ – автоморфизм представления φ. По лемме Шура $\Psi^{-1} \circ \Phi = \lambda\mathcal{E}$, поэтому $\Phi = \lambda\Psi$. □

Еще одно следствие леммы Шура сформулируем в виде следующей теоремы:

Теорема 5.10. *Если группа G абелева, а поле K алгебраически замкнуто, то неприводимые над K представления группы G одномерны.*

Доказательство. Поскольку группа абелева, все операторы представления перестановочны между собой, а, значит, каждый из них является эндоморфизмом представления. По лемме Шура получается, что все $\varphi(g)$ скалярны. Поэтому любое подпространство является инвариантным и поэтому представление неприводимо только если оно одномерно. □

Алгебраическая замкнутость поля существенна. Например, у $G = \mathbb{Z}_n$ есть одномерное комплексное представление $\varphi : G \to \mathbb{C} = \mathbb{R}^2$, $\varphi(\bar{1}) = e^{2\pi i/n}$, которое является неприводимым двумерным представлением над полем $\mathbb{R}$. Как представление над полем $\mathbb{C}$ оно, разумеется, неприводимо, поскольку одномерно над $\mathbb{C}$.

Все неприводимые комплексные представления конечно порожденной абелевой группы легко описать. Пусть

$$G = \mathbb{Z}^k \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_m},$$

где $\mathbb{Z}^k = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ – прямая сумма k слагаемых. Обозначим через $a_1, \ldots, a_k$ образующие бесконечных циклических групп и через $b_1, \ldots, b_m$ образующие групп $Z_{n_1}, \ldots, \mathbb{Z}_{n_m}$. Чтобы задать гомоморфизм $G \to GL(1, \mathbb{C}) = \mathbb{C}^*$ нужно только указать куда переходят образующие. Образующие a_i можно перевести в произвольные ненулевые комплексные числа, а образующая b_j должна переходить в какой-либо корень степени n_j из едидиницы. Такое отображение множества образующих в $\mathbb{C}^*$ однозначно продолжается до гомоморфизма $G \to \mathbb{C}^*$. Видно, что если абелева группа G конечна, то у нее будет ровно $|G|$ различных комплексных представлений.

Обсудим теперь вопрос как построить одномерные представления неабелевой группы.

Предложение 5.11. *Для любого одномерного представления $\varphi : G \to GL(1, K) = K^*$ группы G над произвольным полем K коммутант группы G содержится в ядре гомоморфизма φ.*

Доказательство. Для любых элементов $a, b \in G$ имеем $\varphi([a, b]) = [\varphi(a), \varphi(b)] = 1 \in K^*$, поскольку K^* – абелева группа. □

Таким образом, чтобы построить все одномерные представления группы G мы можем взять факторгруппу группы G по ее коммутанту и построить все одномерные представления этой абелевой группы. В случае конечной порожденности этой абелевой группы как найти все ее комплексные одномерные представления описано выше.

5.1 Некоторые конструкции с представлениями

Если есть представления в векторных пространствах над полем K

$$\varphi_i : G \to GL(V_i), \quad i = 1, \ldots, m,$$

то их *тензорное произведение*

$$\varphi = \varphi_1 \otimes \ldots \otimes \varphi_m$$

определяется следующим образом:

$$\varphi : G \to GL(V), \quad V = V_1 \otimes \ldots \otimes V_m, \quad \varphi(g)(v_1 \otimes \ldots \otimes v_m) := \varphi_1(g)(v_1) \otimes \ldots \otimes \varphi_m(g)(v_m).$$

Более общо: если есть представления групп $\varphi_i : G_i \to GL(V_i)$, $i = 1, \ldots, m$, то их *тензорное произведение*

$$\varphi = \varphi_1 \otimes \ldots \otimes \varphi_m : G \to GL(V), \quad G := G_1 \times \cdots \times G_m, \quad V := V_1 \otimes \ldots \otimes V_m,$$

определяется так:

$$\varphi((g_1, \ldots, g_m))(v_1 \otimes \ldots \otimes v_m) := \varphi_1(g_1)(v_1) \otimes \ldots \otimes \varphi_m(g_m)(v_m).$$

Двойственное пространство V^* (пространство ковекторов, пространство линейных функционалов) определяется как пространство линейных отображений из V в поле K:

$$V^* := \mathrm{Hom}\,(V, K) := \mathrm{Hom}_K(V, K).$$

Пусть $A : V \to V$ – линейный оператор, т.е.

$$A \in \mathrm{Hom}\,(V, V) := \mathrm{Hom}_K(V, V) = \mathrm{End}\ V = L(V).$$

Тогда по нему можно определить линейный оператор ${}^tA : V^* \to V^*$ на двойственном пространстве V^*. Таким образом, ${}^tA \in L(V^*)$. Оператор ${}^tA$, $\eta \mapsto {}^tA\eta$, определяется следующим образом:

$$({}^tA\eta)(v) := \eta(Av).$$

Более общо: пусть $A : V \to W$ – линейное отображение, $v \mapsto Av$, т.е.

$$A \in \mathrm{Hom}\,(V, W) := \mathrm{Hom}_K(V, W).$$

Тогда с помощью A строится линейное отображение ${}^tA : W^* \to V^*$, $\eta \mapsto A\eta$:

$$({}^tA\eta)(v) := \eta(Av), \quad v \in V, \quad \eta \in W^*,$$

что с помощью естественного спаривания

$$\langle \cdot\,, \cdot \rangle : V^* \times V \to K, \quad (\eta, v) \mapsto \langle \eta, v \rangle := \eta(v),$$

можно записать как:

$$\langle {}^tA\eta, v \rangle = \langle \eta, Av \rangle.$$

Последовательность линейных отображений

$$V \xrightarrow{A} W \xrightarrow{B} U$$

индуцирует последовательность линейных отображений двойственных пространств

$$V^* \xleftarrow{{}^tA} W^* \xleftarrow{{}^tB} U^*.$$

Если $v \in V$, $\xi \in U^*$, то

$$\langle ({}^tA \circ {}^tB)\xi, v\rangle = \langle {}^tA({}^tB)\xi, v\rangle = \langle {}^tB\xi, Av\rangle = \langle \xi, B(Av)\rangle = \langle \xi, (B \circ A)v\rangle = \langle {}^t(B \circ A)\xi, v\rangle,$$

откуда следует, что

$${}^t(B \circ A) = {}^tA \circ {}^tB.$$

Представление $\varphi : G \to GL(V)$ индуцирует представление $\varphi^* : G \to GL(V^*)$,

$$\varphi^*(g) := {}^t\varphi(g^{-1}) : V^* \to V^*.$$

Дествительно,

$$\varphi^*(gh) = {}^t\varphi((gh)^{-1}) = {}^t\varphi((h)^{-1}(g)^{-1}) = {}^t[\varphi((h)^{-1})\varphi((g)^{-1})] = {}^t\varphi((g)^{-1})\,{}^t\varphi((h)^{-1}) = \varphi^*(g)\varphi^*(h).$$

Кроме того,

$$\langle \varphi^*(g)\eta, \varphi(g)v\rangle = \langle \eta, v\rangle.$$

Представление $\varphi : G \to GL(V)$ индуцирует представление $\varphi^* : G \to GL(V^*)$ и тем самым дает представления $\varphi \otimes \cdots \otimes \varphi \otimes \varphi^* \otimes \cdots \otimes \varphi^*$ в пространствах тензоров $V \otimes \cdots \otimes V \otimes V^* \otimes \cdots \otimes V^*$. Например, возникает представление группы G в пространстве $L(V) = \operatorname{End} V = \operatorname{Hom}_K(V, V) = V^* \otimes V$. Это представление совпадает с представлением $\sigma \mapsto \varphi(g)\sigma = \varphi(g) \circ \sigma$, $\sigma \in L(V)$.

5.2 Усреднение

Далее предполагается, что G – конечная группа.

Пусть V – комплексное векторное пространство и $(\cdot\,,\,\cdot)$ – эрмитова положительно определенная билинейная форма. Это означает, что

1. $(u, v) \in \mathbb{C}$
$(au + bv, w) = a(u, w) + b(v, w)$, $\forall\, a, b \in \mathbb{C}$, $\forall\, u, v, w \in V$,
2. $(u, v) = \overline{(v, u)}$,
3. $(u, u) \geq 0$ $\forall u \in V$ и $(u, u) = 0 \Leftrightarrow u = 0$.

Из свойств 1 и 2 следует, что

$$(u, av + bw) = \bar{a}(u, v) + \bar{b}(u, w),\ \forall\, a, b \in \mathbb{C},\ \forall\, u, v, w \in V.$$

Отметим также, что из свойства 2 вытекает, что $(u, u) \in \mathbb{R}$ $\forall\, u \in V$.

Положим

$$\langle u, v\rangle := \frac{1}{|G|}\sum_{g\in G}(gu, gv) = \frac{1}{|G|}\sum_{g\in G}(\varphi(g)u, \varphi(g)v).$$

Легко видеть, что получается эрмитова положительно определенная билинейная форма, инвариантная относительно G-действия:

$$\langle gu, gv\rangle = \langle \varphi(g)u, \varphi(g)v\rangle = \langle u, v\rangle.$$

Действительно, покажем, что $\langle hu, hv\rangle = \langle u, v\rangle$ для любого $h \in G$. Имеем:

$$\langle hu, hv\rangle = \frac{1}{|G|}\sum_{g\in G}(ghu, ghv) = \frac{1}{|G|}\sum_{g\in G}(gu, gv) = \langle u, v\rangle.$$

Суммы одинаковы, поскольку когда g пробегает всю группу G, элемент gh тоже пробегает всю группу.

Если форма $(\cdot\,,\,\cdot)$ изначально была инвариантной относительно G-действия, то она совпадает с построенной по ней формой $\langle\cdot\,,\,\cdot\rangle$. Действительно,

$$\langle u, v\rangle = \frac{1}{|G|}\sum_{g\in G}(gu, gv) = \frac{1}{|G|}\sum_{g\in G}(u, v) = \frac{1}{|G|}\cdot|G|\cdot(u, v) = (u, v).$$

Итак мы получили:

Предложение 5.12. *Всякое комплексное (вещественное) линейное конечномерное представление конечной группы эквивалентно унитарному (соответственно ортогональному) представлению.*

Таким образом, без ограничения общности можно считать, что такое представление – это гомоморфизм $G \to U(n)$ (соответственно $G \to O(n)$).

Теорема 5.13. *Любое комплексное (вещественное) конечномерное представление конечной группы вполне приводимо.*

Доказательство. Если $U \subset V$ – инвариантное подпространство, его ортогональное дополнение относительно G-инвариантной формы тоже будет G-инвариантным подпространством. Следовательно, $V = U \oplus U^{\perp}$ – прямая сумма инвариантных подпространств, которое можно рассматривать как пространство прямой суммы представлений. Если слагаемые содержат инвариантные подпространства, то их по той же причине можно будет разложить в сумму инвариантных подпространств. Поскольку пространство конечномерно, мы в результате разложим V в сумму неприводимых инвариантных подпространств. □

Пусть $\varphi : G \to GL(V)$, $\psi : G \to GL(W)$ – представления. Тогда их можно рассматривать как линейные действия группы G:

$$gv = \varphi(g)v,\ v \in V \text{ и } gw = \psi(g)w,\ w \in W,$$

линейность означает, что $g(v_1 + v_2) = gv_1 + gv_2$, $g(\alpha v) = \alpha(gv)$, $v, v_1, v_2 \in V$, $\alpha \in K$, и аналогичные равенства для действия группы G на W.

Пусть $A : V \to W$ – линейное отображение, тогда если порядок группы не равен нулю в поле K, то по A можно построить морфизм представлений A_{av} (индекс

происходит от слова average), который совпадает с A в случае, когда линейное отображение A само является морфизмом представлений, т.е. является линейным эквивариантным отображением.

$$A_{\mathrm{av}} : V \to W, \quad A_{\mathrm{av}} v := \frac{1}{|G|} \sum_{g \in G} \psi(g) A \varphi(g^{-1}) v = \frac{1}{|G|} \sum_{g \in G} g A g^{-1} v = \frac{1}{|G|} \sum_{g \in G} g^{-1} A g v.$$

Используя усреднение линейного отображения можно доказать следующую теорему, обобщающую утверждение о полной приводимости комплексных представлений.

Теорема 5.14 (Машке)**.** *Если $|G| \neq 0$ в поле K, то любое конечномерное представление группы G вполне приводимо.*

Доказательство. Нужно показать только, что инвариантное подпространство выделяется так, что его прямое дополнение тоже инвариантно. Пусть $U \subset V$ – инвариантное подпространство, возьмем произвольное подпространство U', такое, что $V = U \oplus U'$. Возьмем проекцию $A : V \to U$. Тогда $A|_U = \mathrm{id}\, U$. Усредненный оператор A_{av} эквивариантен, $A_{\mathrm{av}}|_U = \mathrm{id}\, U$ и его ядро – искомое дополнительное к U инвариантное подпространство. □

Дальше будут рассматриваться только комплексные представления.

Предложение 5.15. *Пусть $\varphi : G \to GL(V)$, $\psi : G \to GL(W)$ – неприводимые комплексные представления и $A : V \to W$ – произвольное линейное отображение. Тогда его усреднение A_{av} обладает следующими свойствами:*

1) если представления неэквивалентны, то $A_{\mathrm{av}} = 0$,

2) если $V = W$ и $\varphi = \psi$, то $A_{\mathrm{av}} = \lambda E = \lambda\, \mathrm{id}_V$, где $\lambda = \mathrm{tr}\, A / \dim V$.

Доказательство. Оба утверждения сразу следуют из леммы Шура, константа во втором утверждении находится из следующего вычисления:

$$\mathrm{tr}\, \lambda E = \lambda \dim V = \mathrm{tr}\, A_{\mathrm{av}} = \mathrm{tr} \left(\frac{1}{|G|} \sum_{g \in G} \varphi(g) A \varphi(g^{-1}) \right) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\, \varphi(g) A \varphi(g^{-1}) =$$

$$= \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\, \varphi(g) A \varphi(g)^{-1} = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\, A = \frac{1}{|G|} \cdot |G| \cdot \mathrm{tr}\, A = \mathrm{tr}\, A \quad \Rightarrow \quad \lambda \dim V = \mathrm{tr}\, A.$$

□

Если выбрать базисы в V и W, то мы можем переписать полученные соотношения в матричной форме. А именно, будем считать, что $A = (a_{ij})$, A_{av}, $\varphi(g)$, $\psi(g)$ записаны матрицами. Тогда соотношения для неизоморфных неприводимых представлений φ и ψ из предыдущего предложения можно записать следующим образом:

$$(A_{\mathrm{av}})_{ij} = \frac{1}{|G|} \sum_{g \in G} \sum_{l,k} \psi(g)_{il} a_{lk} \varphi(g^{-1})_{kj} = 0,$$

и поскольку a_{ij} можно брать любыми, получаем следующее равенство

$$\frac{1}{|G|}\sum_{g\in G}\psi(g)_{il}\varphi(g^{-1})_{kj}=0$$

для всех i,j,k,l.

Во втором случае, когда $\varphi=\psi$, то $A_{\mathrm{av}}=\lambda E=\lambda\,\mathrm{id}_V$, где $\lambda=\operatorname{tr}A/\dim V$, получаем

$$(A_{\mathrm{av}})_{ij}=\lambda\delta_{ij}=\frac{1}{\dim V}\delta_{ij}\sum_{l,k}\delta_{lk}a_{lk}=\frac{1}{|G|}\sum_{g\in G}\sum_{l,k}\varphi(g)_{il}a_{lk}\varphi(g^{-1})_{kj},$$

и приравнивая коэффициенты при a_{lk} находим

$$\frac{1}{|G|}\sum_{g\in G}\varphi(g)_{il}\varphi(g^{-1})_{kj}=\frac{1}{\dim V}\delta_{ij}\delta_{lk}.$$

Следствие 5.16 (Соотношения ортогональности)**.** *Пусть $\varphi:G\to GL(V)$ и $\psi:G\to GL(W)$ – неприводимые комплексные представления.*

1) Если представления не являются изоморфными, то

$$\frac{1}{|G|}\sum_{g\in G}\psi(g)_{il}\varphi(g^{-1})_{kj}=0$$

для всех i,j,k,l.

2) если $V=W$ и $\varphi=\psi$, то

$$\frac{1}{|G|}\sum_{g\in G}\varphi(g)_{il}\varphi(g^{-1})_{kj}=\frac{1}{\dim V}\delta_{ij}\delta_{lk}=\begin{cases}\dfrac{1}{\dim V}, & \text{если } i=j,\ l=k,\\ 0 & \text{в остальных случаях.}\end{cases}$$

5.3 Характеры

Пусть A,B,C – квадратные матрицы одного и того же размера с элементами из поля K и матрица C невырождена. Тогда

$$\operatorname{tr}AB=\operatorname{tr}BA,\quad \operatorname{tr}C^{-1}AC=\operatorname{tr}A,$$

где tr – след матрицы.

Определение 5.17. *Характер представления $\varphi:G\to GL(V)$* – это комплекснозначная функция на группе

$$\chi_\varphi:G\to\mathbb{C},\qquad \chi_\varphi(g):=\operatorname{tr}\varphi(g).$$

Так как $\varphi(e) = \mathrm{id}_V$, имеем $\chi_\varphi(e) = \dim V = \dim_{\mathbb{C}} V$.

Характер – *центральная функция*, т.е. функция постоянная на классах сопряженных элементов, поскольку

$$\chi_\varphi(h^{-1}gh) = \operatorname{tr}\varphi(h^{-1}gh) = \operatorname{tr}\varphi(h^{-1})\varphi(g)\varphi(h) = \operatorname{tr}\varphi(h)^{-1}\varphi(g)\varphi(h) = \operatorname{tr}\varphi(g) = \chi_\varphi(g).$$

Комплексно-значные центральные функции на группе образуют подпространство в пространстве $\mathbb{C}^G$ всех комплексно-значных функций на группе G. Размерность этого подпространства равна числу классов сопряженных элементов (размерность пространства $\mathbb{C}^G$ всех функций равна, очевидно, порядку группы $|G|$). Ясно также, что $s : G \to \mathbb{C}$ – центральная функция в том и только том случае, когда

$$s(gh) = s(hg), \ \ \forall\, g, h \in G.$$

Используя свойства следа, центральность характеров представлений легко получить установив приведенное выше соотношение

$$\chi_\varphi(gh) = \operatorname{tr}\varphi(gh) = \operatorname{tr}\varphi(g)\varphi(h) = \operatorname{tr}\varphi(h)\varphi(g) = \operatorname{tr}\varphi(hg) = \chi_\varphi(hg).$$

Если $A : V \to V$ – изоморфизм, определив $\psi(g) := A^{-1}\varphi(g)A$ мы получаем гомоморфизм $\psi : G \to GL(V)$, который представляет собой представление ψ эквивалентное представлению φ. Поскольку у подобных матриц след одинаков, мы получаем, что *характеры эквивалентных представлений равны.*

Предложение 5.18. *Пусть $\varphi : G \to GL(V)$ – комплексное линейное представление. Тогда*

1) $\chi_\varphi(e) = \dim V$,
2) $\chi_\varphi(h^{-1}gh) = \chi_\varphi(g) \ \ \forall g, h \in G$,
3) $\chi_\varphi(g^{-1}) = \overline{\chi_\varphi(g)}$,
4) если $\varphi = \varphi_1 \oplus \varphi_2$ – прямая сумма представлений, то $\chi_\varphi = \chi_{\varphi_1} + \chi_{\varphi_2}$,
5) если $\varphi = \varphi_1 \otimes \varphi_2$ – тензорное произведение представлений, то $\chi_\varphi = \chi_{\varphi_1} \cdot \chi_{\varphi_2}$.

Доказательство. Утверждение 2 было доказано выше. Утверждение 1 очевидно. Утверждения 4, 5 следуют из известных свойств следа. Утверждение 5 следует из того, что представление эквивалентно унитарному, а, значит, можно считать, что матрица $\varphi(g)$ унитарна, а поэтому обратная к ней матрица $\varphi(g^{-1}) = \varphi(g)^{-1}$ получается транспонированием и взятием сопряжения всех элементов. Тем самым диагональные элементы матриц $\varphi(g)$ и $\varphi(g^{-1})$ сопряжены, а, следовательно и следы этих матриц сопряжены. □

Определим эрмитову положительно определенную форму на пространстве комплексно-значных функций на группе G следующим образом: для $s, t \in \mathbb{C}^G$ положим

$$(s, t) = \frac{1}{|G|} \sum_{g \in G} s(g)\overline{t(g)}.$$

Если упорядочить элементы группы G и сопоставить комплексно-значной функции на группе ее вектор значений, то получим изоморфизм $\mathbb{C}^G \cong \mathbb{C}^n$ векторных пространств над полем комплексных чисел, где $n = |G|$. Введенное выше эрмитово скалярное произведение на $\mathbb{C}^G$ дает скалярное произведение на $\mathbb{C}^n$, которое в n раз меньше стандартного эрмитова скалярного произведения на $\mathbb{C}^n$.

Теорема 5.19. *Пусть φ, ψ – неприводимые комплексные представления конечной группы G. Если представления эквивалентны, то $(\chi_\varphi, \chi_\psi) = 1$, а если неэквивалентны, то $(\chi_\varphi, \chi_\psi) = 0$, т.е. характеры неэквивалентных неприводимых представлений ортогональны.*

Доказательство. У эквивалентных представлений характеры одинаковы, поэтому первое утверждение будет доказано, если показать, что $(\chi_\varphi, \chi_\varphi) = 1$. Имеем

$$(\chi_\varphi, \chi_\varphi) = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \varphi(g) \overline{\operatorname{tr} \varphi(g)} = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \varphi(g) \operatorname{tr} \varphi(g^{-1}).$$

В матричной записи $\operatorname{tr} \varphi(g) = \sum_i \varphi(g)_{ii}$ и $\operatorname{tr} \varphi(g^{-1}) = \sum_j \varphi(g^{-1})_{jj}$. Поэтому из соотношений ортогональности (см. следствие 5.16) получаем

$$\begin{aligned}(\chi_\varphi, \chi_\varphi) &= \frac{1}{|G|} \sum_{g \in G} \sum_{i,j} \varphi(g)_{ii} \varphi(g^{-1})_{jj} = \\ &= \sum_{i,j} \frac{1}{|G|} \sum_{g \in G} \varphi(g)_{ii} \varphi(g^{-1})_{jj} = \sum_{i,j} \frac{\delta_{ij}}{\dim V} = \sum_i \frac{\delta_{ii}}{\dim V} = 1,\end{aligned}$$

поскольку индекс i пробегает значения от 1 до $\dim V$.

Второе утверждение также доказывается с помощью следствия 5.16. Имеем

$$\begin{aligned}(\chi_\psi, \chi_\varphi) &= \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \psi(g) \overline{\operatorname{tr} \varphi(g)} = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \psi(g) \operatorname{tr} \varphi(g^{-1}) = \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{i,j} \psi(g)_{ii} \varphi(g^{-1})_{jj} = \sum_{i,j} \frac{1}{|G|} \sum_{g \in G} \psi(g)_{ii} \varphi(g^{-1})_{jj} = 0.\end{aligned}$$

□

Теорема 5.20. *Пусть $\varphi : G \to GL(V)$ – линейное представление группы G. Предположим, что V разлагается в прямую сумму неприводимых представлений: $V = W_1 \oplus \cdots \oplus W_k$. Тогда если $\psi : G \to GL(W)$ – некоторое неприводимое представление, то число слагаемых W_i изоморфных представлению W, равно скалярному произведению $(\chi_\varphi, \chi_\psi)$.*

Доказательство. Обозначим через χ_i характер представления W_i, тогда

$$\chi_\varphi = \chi_1 + \cdots + \chi_k \quad \Rightarrow \quad (\chi_\varphi, \chi_\psi) = (\chi_1, \chi_\psi) + \cdots + (\chi_k, \chi_\psi).$$

Поскольку (χ_i, χ_ψ) равно 1, если представления W_i и W изоморфны и равно 0 в противном случае, получаем требуемое. □

Следствие 5.21. *Число неприводимых подпредставлений W_i в V изоморфных данному неприводимому представлению W не зависит от способа разложения.*

(Это число называется кратностью вхождения W в представление V.)

Доказательство. Указанное число равно скалярному произведению характеров представлений V и W, которое не зависит способа разложения. □

Следствие 5.22. *Два представления, имеющие один и тот же характер, изоморфны.*

Доказательство. В самом деле, в силу предыдущего следствия, они содержат одинаковое число раз любое заданное неприводимое представление. □

Таким, образом, два конечномерных комплексных представления конечной группы изоморфны тогда и только тогда, когда их характеры равны.

Рассмотрим групповую алгебру $\mathbb{C}[G]$ как левый модуль над собой. Операторы умножения слева на элементы группы обратимы, поэтому мы получаем представление группы G в комплексном векторном пространстве $\mathbb{C}[G]$. Это представление называется *регулярным представлением.*

Обозначим через χ_{reg} характер регулярного представления. Имеем

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & \text{для } g = e, \\ 0 & \text{для } g \neq e. \end{cases}$$

Действительно, базис в $\mathbb{C}[G]$ состоит из всех элементов группы (упорядоченных каким-либо образом), при действии элемента $g \in G$, $g \neq e$, каждый базисный вектор переходит в некоторый другой базисный вектор, поэтому строки и столбцы матрицы этого оператора состоят из нулей, кроме одного элемента равного 1, причем диагональные элементы все равны нулю, поэтому след такого оператора равен нулю. Наконец, $\chi_{\text{reg}}(e) = \dim \mathbb{C}[G] = |G|$.

Теперь легко найти скалярный квадрат характера регулярного представления:

$$(\chi_{\text{reg}}, \chi_{\text{reg}}) = \frac{1}{|G|} \sum_{g \in G} \chi_{\text{reg}}(g)\overline{\chi_{\text{reg}}(g)} = \frac{1}{|G|} \cdot \chi^2_{\text{reg}}(e) = \frac{1}{|G|} \cdot |G|^2 = |G|,$$

а также скалярное произведение с любым другим характером:

$$(\chi_\varphi, \chi_{\text{reg}}) = \frac{1}{|G|} \sum_{g \in G} \chi_\varphi(g)\overline{\chi_{\text{reg}}(g)} = \frac{1}{|G|} \cdot \chi_\varphi(e)\chi_{\text{reg}}(e) = \frac{1}{|G|} \cdot \dim V \cdot |G| = \dim V,$$

где $\varphi : G \to GL(V)$.

Теорема 5.23. *Пусть $\varphi_1, \ldots, \varphi_m$ – все неприводимые комплексные представления конечной группы G, $\varphi_i : G \to GL(V_i)$. Тогда каждое неприводимое представление φ_i входит в разложение регулярного представления с кратностью, равной его размерности $n_i = \dim V_i$ и $|G| = \sum_{i=1}^m n_i^2$.*

Доказательство. Предположим, что регулярное представление изоморфно представлению $l_1\varphi_1 \oplus \cdots \oplus l_m\varphi_m$. Тогда

$$\chi_{\text{reg}} = l_1\chi_{\varphi_1} + \cdots + l_m\chi_{\varphi_m} \quad \Rightarrow \quad (\chi_{\text{reg}}, \chi_{\varphi_i}) = l_i, \;\; i = 1, \ldots, m.$$

С другой стороны, $(\chi_{\text{reg}}, \chi_{\varphi_i}) = \dim V_i = n_i \;\Rightarrow\; l_i = n_i$.

Для доказательства равенства $|G| = \sum_{i=1}^m n_i^2$ заметим, что левая часть равенства равна $(\chi_{\text{reg}}, \chi_{\text{reg}})$. Поскольку регулярное представление изоморфно представлению $n_1\varphi_1 \oplus \cdots \oplus n_m\varphi_m$, его скалярный квадрат $(\chi_{\text{reg}}, \chi_{\text{reg}})$ равен $\sum_{i=1}^m n_i^2$, что доказывается с использованием равенств

$$(\chi_{\varphi_i}, \chi_{\varphi_i}) = 1,\ i = 1, \ldots, m, \text{ и } (\chi_{\varphi_i}, \chi_{\varphi_j}) = 0 \text{ при } i \neq j.$$

□

Предложение 5.24. *Характеры всех попарно неэквивалентных неприводимых комплексных представлений конечной группы образуют ортонормированный базис пространства всех центральных комплексно-значных функций на группе.*

Теорема 5.25. *Число неприводимых комплексных представлений конечной группы G (с точностью до изоморфизма) равно числу ее классов сопряженных элементов.*

Пусть $V_1, \ldots, V_m$ – пространства всех неприводимых представлений $\varphi_1, \ldots, \varphi_m$ конечной группы G. Тогда любое конечномерное представление $\psi : G \to GL(V)$ эквивалентно сумме $n_1\varphi_1 \oplus \cdots \oplus n_m\varphi_m$ и V изоморфно сумме $n_1V_1 \oplus \cdots \oplus n_mV_m$. При этом если разложить в сумму неприводимых и собрать изоморфные слагаемые в группы, то разложение в сумму таких групп будет однозначным. Оно называется *каноническим разложением представления*. Числа n_i можно найти взяв скалярное произведение характеров представлений φ и φ_i:

$$n_i = (\chi_\varphi, \chi_{\varphi_i}).$$

Теорема 5.26. *Пусть $\varphi_1 : G_1 \to V_1$, $\varphi_2 : G_2 \to V_2$ – линейные представления групп G_1 и G_2, и пусть $\varphi := \varphi_1 \otimes \varphi_2 : G = G_1 \times G_2 \to GL(V_1 \otimes V_2)$ – тензорное произведение этих представлений. Тогда $\chi_\varphi((g_1, g_2)) = \chi_{\varphi_1}(g_1) \cdot \chi_{\varphi_2}(g_2)$.*

Представление $\varphi = \varphi_1 \otimes \varphi_2$ неприводимо тогда и только тогда, когда неприводимы представления φ_1, φ_2.

Доказательство. Имеем

$$\chi_\varphi((g_1, g_2)) = \operatorname{tr}(\varphi_1(g_1) \otimes \varphi_2(g_2)) = \operatorname{tr}\varphi_1(g_1) \cdot \operatorname{tr}\varphi_2(g_2) = \chi_{\varphi_1}(g_1) \cdot \chi_{\varphi_2}(g_2).$$

Мы докажем только, что тензорное произведение неприводимых представлений является неприводимым.

Представление $\varphi := \varphi_1 \otimes \varphi_2$ неприводимо $\Leftrightarrow (\chi_\varphi, \chi_\varphi) = 1$. Поэтому утверждение о его неприводимости вытекает из соотношения

$$(\chi_\varphi, \chi_\varphi) = (\chi_{\varphi_1}, \chi_{\varphi_1}) \cdot (\chi_{\varphi_2}, \chi_{\varphi_2}),$$

которое доказывается прямым вычислением:

$$(\chi_\varphi, \chi_\varphi) = \frac{1}{|G|} \sum_{(g_1,g_2)\in G} \chi_\varphi((g_1,g_2))\overline{\chi_\varphi((g_1,g_2))} =$$
$$= \frac{1}{|G_1|}\frac{1}{|G_2|} \sum_{(g_1,g_2)\in G} \chi_{\varphi_1}(g_1)\cdot\chi_{\varphi_2}(g_2)\overline{\chi_{\varphi_1}(g_1)}\cdot\overline{\chi_{\varphi_2}(g_2)} =$$
$$= \left(\frac{1}{|G_1|}\sum_{g_1\in G_1}\chi_{\varphi_1}(g_1)\overline{\chi_{\varphi_1}(g_1)}\right)\cdot\left(\frac{1}{|G_2|}\sum_{g_2\in G_2}\chi_{\varphi_2}(g_2)\overline{\chi_{\varphi_2}(g_2)}\right) = (\chi_{\varphi_1},\chi_{\varphi_1})\cdot(\chi_{\varphi_2},\chi_{\varphi_2}).$$

□

Пример 5.27. Найдем все комплексные неприводимые представления группы $S_3 = D_3$. У этой группы имеются два одномерных неприводимых представления – тривиальное представление (каждый элемент группы S_3 отправляется в $1 \in \mathbb{C}^* = GL(1,\mathbb{C})$) и представление, относящее подстановке ее знак.

Имеется еще одно двумерное неприводимое представление. Чтобы его писать вспомним как определялась группа D_3. Она порождается двумя элементами a и b, которые $\mathbb{R}$-линейно действуют на $\mathbb{C}$ следующим образом: a – поворот на угол $2\pi/3$ против часовой стрелки (т.е. a действует умножением на $e^{\frac{2\pi i}{3}}$), а b – сопряжение. Получается неприводимое вещественное двумерное представление. Его комплексификация даст двумерное неприводимое комплексное представление. Это означает, что если обозначить через e_1, e_2 базис в $\mathbb{C}^2$, то
$be_1 = e_1, be_2 = -e_2, ae_1 = \cos(2\pi/3)e_1 + \sin(2\pi/3)e_2, ae_2 = -\sin(2\pi/3)e_1 + \cos(2\pi/3)e_2$.
Получается двумерное комплексное неприводимое представление. Поскольку

$$|S_3| = 6 = 1^2 + 1^2 + 2^2,$$

других неприводимых представлений, кроме перечисленных, нет. Можно этот факт также обосновать тем, что число классов сопряженных элементов группы S_3 равно 3 (оно равно числу цикленных типов подстановок; нетривиальных класса два – класс элементов, сопряженных с танспозицией, скажем $(1,2)$, и класс элементов, сопряженных с циклом $(1,2,3)$).