s

Лекции курса «Алгебра», лекторы И. В. Аржанцев и Р. С. Авдеев

ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2015/2016 учебный год

Содержание

Лекция 1

Полугруппы и группы: основные определения и примеры. Группы подстановок и группы матриц. Подгруппы. Порядок элемента и циклические подгруппы. Смежные классы и индекс подгруппы. Теорема Лагранжа.

Определение 1. *Множество с бинарной операцией* — это множество M с заданным отображением

$$M \times M \to M, \quad (a,b) \mapsto a \circ b.$$

Множество с бинарной операцией обычно обозначают $(M, \circ)$.

Определение 2. Множество с бинарной операцией $(M, \circ)$ называется *полугруппой*, если данная бинарная операция *ассоциативна*, т. е.

$$a \circ (b \circ c) = (a \circ b) \circ c \quad \text{для всех } a, b, c \in M.$$

Не все естественно возникающие операции ассоциативны. Например, если $M = \mathbb{N}$ и $a \circ b := a^b$, то

$$2^{(1^2)} = 2 \neq (2^1)^2 = 4.$$

Другой пример неассоциативной бинарной операции: $M = \mathbb{Z}$ и $a \circ b := a - b$ (проверьте!).

Полугруппу обычно обозначают $(S, \circ)$.

Определение 3. Полугруппа $(S, \circ)$ называется *моноидом*, если в ней есть *нейтральный элемент*, т. е. такой элемент $e \in S$, что $e \circ a = a \circ e = a$ для любого $a \in S$.

Во Франции полугруппа $(\mathbb{N}, +)$ является моноидом, а в России нет.

Замечание 1. Если в полугруппе есть нейтральный элемент, то он один. В самом деле, $e_1 \circ e_2 = e_1 = e_2$.

Определение 4. Моноид $(S, \circ)$ называется *группой*, если для каждого элемента $a \in S$ найдется *обратный элемент*, т. е. такой $b \in S$, что $a \circ b = b \circ a = e$.

Упражнение 1. Докажите, что если обратный элемент существует, то он один.

Обратный элемент обозначается a^{-1}. Группу принято обозначать $(G, \circ)$ или просто G, когда понятно, о какой операции идёт речь. Обычно символ $\circ$ для обозначения операции опускают и пишут просто ab.

Определение 5. Группа G называется *коммутативной* или *абелевой*, если групповая операция *коммутативна*, т. е. $ab = ba$ для любых $a, b \in G$.

Если в случае произвольной группы G принято использовать мультипликативные обозначения для групповой операции — gh, e, g^{-1}, то в теории абелевых групп чаще используют аддитивные обозначения, т. е. $a + b$, 0, $-a$.

Определение 6. *Порядок* группы G — это число элементов в G. Группа называется *конечной*, если её порядок конечен, и *бесконечной* иначе.

Порядок группы G обозначается $|G|$.

Приведём несколько серий примеров групп.

1) Числовые аддитивные группы: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}_n, +)$.

2) Числовые мультипликативные группы: $(\mathbb{Q} \setminus \{0\}, \times)$, $(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C} \setminus \{0\}, \times)$, $(\mathbb{Z}_p \setminus \{\overline{0}\}, \times)$, p — простое.

3) Группы матриц: $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}(n \times n, \mathbb{R}) \mid \det(A) \neq 0\}$; $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}(n \times n, \mathbb{R}) \mid \det(A) = 1\}$.

4) Группы подстановок: симметрическая группа S_n — все подстановки длины n, $|S_n| = n!$;

знакопеременная группа A_n — чётные подстановки длины n, $|A_n| = n!/2$.

Упражнение 2. Докажите, что группа S_n коммутативна $\Leftrightarrow n \leqslant 2$, а A_n коммутативна $\Leftrightarrow n \leqslant 3$.

Определение 7. Подмножество H группы G называется *подгруппой*, если выполнены следующие три условия: (1) $e \in H$; (2) $ab \in H$ для любых $a, b \in H$; (3) $a^{-1} \in H$ для любого $a \in H$.

Упражнение 3. Проверьте, что H является подгруппой тогда и только тогда, когда H непусто и $ab^{-1} \in H$ для любых $a, b \in H$.

В каждой группе G есть *несобственные* подгруппы $H = \{e\}$ и $H = G$. Все прочие подгруппы называются *собственными*. Например, чётные числа $2\mathbb{Z}$ образуют собственную подгруппу в $(\mathbb{Z}, +)$.

Предложение 1. *Всякая подгруппа в* $(\mathbb{Z}, +)$ *имеет вид* $k\mathbb{Z}$ *для некоторого целого неотрицательного* k.

Доказательство. Пусть H — подгруппа в $\mathbb{Z}$. Если $H = \{0\}$, положим $k = 0$. Иначе пусть k — наименьшее натуральное число, лежащее в H (почему такое есть?). Тогда $k\mathbb{Z} \subseteq H$. С другой стороны, если $a \in H$ и $a = qk + r$ — результат деления a на k с остатком, то $0 \leqslant r \leqslant k - 1$ и $r = a - qk \in H$. Отсюда $r = 0$ и $H = k\mathbb{Z}$. □

Определение 8. Пусть G — группа и $g \in G$. *Циклической подгруппой*, порождённой элементом g, называется подмножество $\{g^n \mid n \in \mathbb{Z}\}$ в G.

Циклическая подгруппа, порождённая элементом g, обозначается $\langle g \rangle$. Элемент g называется *порождающим* или *образующим* для подгруппы $\langle g \rangle$. Например, подгруппа $2\mathbb{Z}$ в $(\mathbb{Z}, +)$ является циклической, и в качестве порождающего элемента в ней можно взять $g = 2$ или $g = -2$. Другими словами, $2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$.

Определение 9. Пусть G — группа и $g \in G$. *Порядком* элемента g называется такое наименьшее натуральное число m, что $g^m = e$. Если такого натурального числа m не существует, говорят, что порядок элемента g равен бесконечности.

Порядок элемента обозначается $\operatorname{ord}(g)$. Заметим, что $\operatorname{ord}(g) = 1$ тогда и только тогда, когда $g = e$.

Следующее предложение объясняет, почему для порядка группы и порядка элемента используется одно и то же слово.

Предложение 2. *Пусть* G *— группа и* $g \in G$. *Тогда* $\operatorname{ord}(g) = |\langle g \rangle|$.

Доказательство. Заметим, что если $g^k = g^s$, то $g^{k-s} = e$. Поэтому если элемент g имеет бесконечный порядок, то все элементы g^n, $n \in \mathbb{Z}$, попарно различны, и подгруппа $\langle g \rangle$ содержит бесконечно много элементов. Если же порядок элемента g равен m, то из минимальности числа m следует, что элементы $e = g^0, g = g^1, g^2, \ldots, g^{m-1}$ попарно различны. Далее, для всякого $n \in \mathbb{Z}$ мы имеем $n = mq + r$, где $0 \leqslant r \leqslant m - 1$, и

$$g^n = g^{mq+r} = (g^m)^q g^r = e^q g^r = g^r.$$

Следовательно, $\langle g \rangle = \{e, g, \ldots, g^{m-1}\}$ и $|\langle g \rangle| = m$. □

Определение 10. Группа G называется *циклической*, если найдётся такой элемент $g \in G$, что $G = \langle g \rangle$.

Ясно, что любая циклическая группа коммутативна и не более чем счётна. Примерами циклических групп являются группы $(\mathbb{Z}, +)$ и $(\mathbb{Z}_n, +)$, $n \geq 1$.

Перейдем ещё к одному сюжету, связанному с парой группа–подгруппа.

Определение 11. Пусть G — группа, $H \subseteq G$ — подгруппа и $g \in G$. *Левым смежным классом* элемента g группы G по подгруппе H называется подмножество

$$gH = \{gh \mid h \in H\}.$$

Лемма 1. *Пусть* G *— группа,* $H \subseteq G$ *— её подгруппа и* $g_1, g_2 \in G$. *Тогда либо* $g_1H = g_2H$, *либо* $g_1H \cap g_2H = \varnothing$.

Доказательство. Предположим, что $g_1H \cap g_2H \neq \varnothing$, т. е. $g_1h_1 = g_2h_2$ для некоторых $h_1, h_2 \in H$. Нужно доказать, что $g_1H = g_2H$. Заметим, что $g_1H = g_2h_2h_1^{-1}H \subseteq g_2H$. Обратное включение доказывается аналогично. □

Лемма 2. *Пусть* G *— группа и* $H \subseteq G$ *— конечная подгруппа. Тогда* $|gH| = |H|$ *для любого* $g \in G$.

Доказательство. Поскольку $gH = \{gh \mid h \in H\}$, в $|gH|$ элементов не больше, чем в H. Если $gh_1 = gh_2$, то домножаем слева на g^{-1} и получаем $h_1 = h_2$. Значит, все элементы вида gh, где $h \in H$, попарно различны, откуда $|gH| = |H|$. □

Определение 12. Пусть G — группа и $H \subseteq G$ — подгруппа. *Индексом* подгруппы H в группе G называется число левых смежных классов G по H.

Индекс группы G по подгруппе H обозначается $[G : H]$.

Теорема Лагранжа. Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда

$$|G| = |H| \cdot [G : H].$$

Доказательство. Каждый элемент группы G лежит в (своём) левом смежном классе по подгруппе H, разные смежные классы не пересекаются (лемма 1) и каждый из них содержит по $|H|$ элементов (лемма 2). $\square$

На следующей лекции мы обсудим следствия из данной теоремы.

Лекция 2

Следствия из теоремы Лагранжа. Нормальные подгруппы. Факторгруппы и теорема о гомоморфизме. Прямое произведение групп. Разложение конечной циклической группы.

Рассмотрим некоторые следствия из теоремы Лагранжа.

Следствие 1. *Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда $|H|$ делит $|G|$.*

Следствие 2. *Пусть G — конечная группа и $g \in G$. Тогда $\operatorname{ord}(g)$ делит $|G|$.*

Доказательство. Это вытекает из следствия 1 и предложения 2 прошлой лекции. □

Следствие 3. *Пусть G — конечная группа и $g \in G$. Тогда $g^{|G|} = e$.*

Доказательство. Согласно следствию 2, мы имеем $|G| = \operatorname{ord}(g) \cdot s$, откуда $g^{|G|} = (g^{\operatorname{ord}(g)})^s = e^s = e$. □

Следствие 4. *Пусть G — группа. Предположим, что $|G|$ — простое число. Тогда G — циклическая группа, порождаемая любым своим неединичным элементом.*

Доказательство. Пусть $g \in G$ — произвольный неединичный элемент. Тогда циклическая подгруппа $\langle g \rangle$ содержит более одного элемента и $|\langle g \rangle|$ делит $|G|$ по следствию 1. Значит, $|\langle g \rangle| = |G|$, откуда $G = \langle g \rangle$. □

Наряду с левым смежным классом можно определить *правый смежный класс* элемента g группы G по подгруппе H:

$$Hg = \{hg \mid h \in H\}.$$

Повторяя доказательство теоремы Лагранжа для правых смежных классов, мы получим, что для конечной группы G число правых смежных классов по подгруппе H равно числу левых смежных классов и равно $|G|/|H|$. В то же время равенство $gH = Hg$ выполнено не всегда. Разумеется, оно выполнено, если группа G абелева. Подгруппы H (неабелевых) групп G, для которых $gH = Hg$ выполнено для любого $g \in G$, будут изучаться в следующей лекции.

Определение 13. Подгруппа H группы G называется *нормальной*, если $gH = Hg$ для любого $g \in G$.

Предложение 3. *Для подгруппы $H \subseteq G$ следующие условия эквивалентны:*
(1) H нормальна;
(2) $gHg^{-1} \subseteq H$ для любого $g \in G$;
(3) $gHg^{-1} = H$ для любого $g \in G$.

Доказательство. (1)⇒(2) Пусть $h \in H$ и $g \in G$. Поскольку $gH = Hg$, имеем $gh = h'g$ для некоторого $h' \in H$. Тогда $ghg^{-1} = h'gg^{-1} = h' \in H$.
(2)⇒(3) Так как $gHg^{-1} \subseteq H$, остаётся проверить обратное включение. Для $h \in H$ имеем $h = gg^{-1}hgg^{-1} = g(g^{-1}hg)g^{-1} \subseteq gHg^{-1}$, поскольку $g^{-1}hg \in H$ в силу пункта (2), где вместо g взято g^{-1}.

(3)⇒(1) Для произвольного $g \in G$ в силу (3) имеем $gH = gHg^{-1}g \subseteq Hg$, так что $gH \subseteq Hg$. Аналогично проверяется обратное включение. □

Условие (2) в этом предложении кажется излишним, но именно его удобно проверять при доказательстве нормальности подгруппы H.

Обозначим через G/H множество (левых) смежных классов группы G по нормальной подгруппе H. На G/H можно определить бинарную операцию следующим образом:

$$(g_1H)(g_2H) := g_1g_2H.$$

Зачем здесь нужна нормальность подгруппы H? Для проверки корректности: заменим g_1 и g_2 другими представителями g_1h_1 и g_2h_2 тех же смежных классов. Нужно проверить, что $g_1g_2H = g_1h_1g_2h_2H$. Это следует из того, что $g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2$ и $g_2^{-1}h_1g_2$ лежит в H.

Ясно, что указанная операция на множестве G/H ассоциативна, обладает нейтральным элементом eH и для каждого элемента gH есть обратный элемент $g^{-1}H$.

Определение 14. Множество G/H с указанной операцией называется *факторгруппой* группы G по нормальной подгруппе H.

Пример 1. Если $G = (\mathbb{Z}, +)$ и $H = n\mathbb{Z}$, то G/H — это в точности группа вычетов $(\mathbb{Z}_n, +)$.

Как представлять себе факторгруппу? В этом помогает теорема о гомоморфизме. Но прежде чем её сформулировать, обсудим ещё несколько понятий.

Определение 15. Пусть G и F — группы. Отображение $\varphi\colon G \to F$ называется *гомоморфизмом*, если $\varphi(ab) = \varphi(a)\varphi(b)$ для любых $a, b \in G$.

Замечание 2. Подчеркнём, что в этом определении произведение ab берётся в группе G, в то время как произведение $\varphi(a)\varphi(b)$ — в группе F.

Лемма 3. *Пусть $\varphi\colon G \to F$ — гомоморфизм групп, и пусть e_G и e_F — нейтральные элементы групп G и F соответственно. Тогда:*

(а) $\varphi(e_G) = e_F$;

(б) $\varphi(a^{-1}) = \varphi(a)^{-1}$ для любого $a \in G$.

Доказательство. (а) Имеем $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$. Теперь умножая крайние части этого равенства на $\varphi(e_G)^{-1}$ (например, слева), получим $e_F = \varphi(e_G)$.

(б) Имеем $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e_G) = e_F$, откуда $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

Определение 16. Гомоморфизм групп $\varphi\colon G \to F$ называется *изоморфизмом*, если отображение φ биективно.

Упражнение 4. Пусть $\varphi\colon G \to F$ — изоморфизм групп. Проверьте, что обратное отображение $\varphi^{-1}\colon F \to G$ также является изоморфизмом.

Определение 17. Группы G и F называют *изоморфными*, если между ними существует изоморфизм.

Обозначение: $G \cong F$ (или $G \simeq F$).

В алгебре группы рассматривают с точностью до изоморфизма: изоморфные группы считаются «одинаковыми».

Определение 18. С каждым гомоморфизмом групп $\varphi\colon G \to F$ связаны его *ядро*

$$\operatorname{Ker}(\varphi) = \{g \in G \mid \varphi(g) = e_F\}$$

и *образ*

$$\operatorname{Im}(\varphi) = \{a \in F \mid \exists g \in G : \varphi(g) = a\}.$$

Ясно, что $\operatorname{Ker}(\varphi) \subseteq G$ и $\operatorname{Im}(\varphi) \subseteq F$ — подгруппы.

Лемма 4. *Гомоморфизм групп $\varphi\colon G \to F$ инъективен тогда и только тогда, когда* $\operatorname{Ker}(\varphi) = \{e_G\}$.

Доказательство. Ясно, что если φ инъективен, то $\operatorname{Ker}(\varphi) = \{e_G\}$. Обратно, пусть $g_1, g_2 \in G$ и $\varphi(g_1) = \varphi(g_2)$. Тогда $g_1^{-1}g_2 \in \operatorname{Ker}(\varphi)$, поскольку $\varphi(g_1^{-1}g_2) = \varphi(g_1^{-1})\varphi(g_2) = \varphi(g_1)^{-1}\varphi(g_2) = e_F$. Отсюда $g_1^{-1}g_2 = e_G$ и $g_1 = g_2$. □

Следствие 5. *Гомоморфизм групп $\varphi\colon G \to F$ является изоморфизмом тогда и только тогда, когда* $\operatorname{Ker}(\varphi) = \{e_G\}$ *и* $\operatorname{Im}(\varphi) = F$.

Предложение 4. *Пусть $\varphi\colon G \to F$ — гомоморфизм групп. Тогда подгруппа* $\operatorname{Ker}(\varphi)$ *нормальна в* G.

Доказательство. Достаточно проверить, что $g^{-1}hg \in \operatorname{Ker}(\varphi)$ для любых $g \in G$ и $h \in \operatorname{Ker}(\varphi)$. Это следует из цепочки равенств

$$\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})e_F\varphi(g) = \varphi(g^{-1})\varphi(g) = \varphi(g)^{-1}\varphi(g) = e_F.$$

□

Теорема о гомоморфизме. Пусть $\varphi\colon G \to F$ — гомоморфизм групп. Тогда группа $\operatorname{Im}(\varphi)$ изоморфна факторгруппе $G/\operatorname{Ker}(\varphi)$.

Доказательство. Рассмотрим отображение $\psi\colon G/\operatorname{Ker}(\varphi) \to F$, заданное формулой $\psi(g\operatorname{Ker}(\varphi)) = \varphi(g)$. Проверка корректности: равенство $\varphi(gh_1) = \varphi(gh_2)$ для любых $h_1, h_2 \in \operatorname{Ker}(\varphi)$ следует из цепочки

$$\varphi(gh_1) = \varphi(g)\varphi(h_1) = \varphi(g) = \varphi(g)\varphi(h_2) = \varphi(gh_2).$$

Отображение ψ сюръективно по построению и инъективно в силу того, что $\varphi(g) = e_F$ тогда и только тогда, когда $g \in \operatorname{Ker}(\varphi)$ (т. е. $g\operatorname{Ker}(\varphi) = \operatorname{Ker}(\varphi)$). Остаётся проверить, что ψ — гомоморфизм:

$$\psi((g\operatorname{Ker}(\varphi))(g'\operatorname{Ker}(\varphi))) = \psi(gg'\operatorname{Ker}(\varphi)) = \varphi(gg') = \varphi(g)\varphi(g') = \psi(g\operatorname{Ker}(\varphi))\psi(g'\operatorname{Ker}(\varphi)).$$

□

Тем самым, чтобы удобно реализовать факторгруппу G/H, можно найти такой гомоморфизм $\varphi\colon G \to F$ в некоторую группу F, что $H = \operatorname{Ker}(\varphi)$, и тогда $G/H \cong \operatorname{Im}(\varphi)$.

Пример 2. Пусть $G = (\mathbb{R}, +)$ и $H = (\mathbb{Z}, +)$. Рассмотрим группу $F = (\mathbb{C} \setminus \{0\}, \times)$ и гомоморфизм

$$\varphi\colon G \to F, \quad a \mapsto e^{2\pi \imath a} = \cos(2\pi a) + i\sin(2\pi a).$$

Тогда $\mathrm{Ker}(\varphi) = H$ и факторгруппа G/H изоморфна окружности S^1, рассматриваемой как подгруппа в F, состоящая из комплексных чисел с модулем 1.

Определим ещё одну важную конструкцию, позволяющую строить новые группы из имеющихся.

Определение 19. *Прямым произведением* групп $G_1, \ldots, G_m$ называется множество

$$G_1 \times \ldots \times G_m = \{(g_1, \ldots, g_m) \mid g_1 \in G_1, \ldots, g_m \in G_m\}$$

с операцией $(g_1, \ldots, g_m)(g_1', \ldots, g_m') = (g_1 g_1', \ldots, g_m g_m')$.

Ясно, что эта операция ассоциативна, обладает нейтральным элементом $(e_{G_1}, \ldots, e_{G_m})$ и для каждого элемента $(g_1, \ldots, g_m)$ есть обратный элемент $(g_1^{-1}, \ldots, g_m^{-1})$.

Замечание 3. Группа $G_1 \times \ldots \times G_m$ коммутативна в точности тогда, когда коммутативна каждая из групп $G_1, \ldots, G_m$.

Замечание 4. Если все группы $G_1, \ldots, G_m$ конечны, то $|G_1 \times \ldots \times G_m| = |G_1| \cdot \ldots \cdot |G_m|$.

Определение 20. Группа G *раскладывается в прямое произведение* своих подгрупп $H_1, \ldots, H_m$, если отображение $H_1 \times \ldots \times H_M \to G$, $(h_1, \ldots, h_m) \mapsto h_1 \cdot \ldots \cdot h_m$ является изоморфизмом.

Лекция 3

Факторизация по сомножителям. Конечно порождённые и свободные абелевы группы. Подгруппы свободных абелевых групп.

Следующий результат связывает конструкции факторгруппы и прямого произведения.

Теорема о факторизации по сомножителям. Пусть $H_1, \ldots, H_m$ — нормальные подгруппы в группах $G_1, \ldots, G_m$ соответственно. Тогда $H_1 \times \ldots \times H_m$ — нормальная подгруппа в $G_1 \times \ldots \times G_m$ и имеет место изоморфизм групп

$$(G_1 \times \ldots \times G_m)/(H_1 \times \ldots \times H_m) \cong G_1/H_1 \times \ldots \times G_m/H_m.$$

Доказательство. Прямая проверка показывает, что $H_1 \times \ldots \times H_m$ — нормальная подгруппа в $G_1 \times \ldots \times G_m$. Требуемый изоморфизм устанавливается отображением

$$(g_1, \ldots, g_m)(H_1 \times \ldots \times H_m) \mapsto (g_1 H_1, \ldots, g_m H_m).$$

□

Теорема 1. *Пусть $n = ml$ — разложение натурального числа n на два взаимно простых множителя. Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_l.$$

Доказательство. Рассмотрим отображение

$$\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_l, \quad k \pmod n \mapsto (k \pmod m, k \pmod l).$$

Поскольку m и l делят n, отображение φ определено корректно. Ясно, что φ — гомоморфизм. Далее, если k переходит в нейтральный элемент $(0,0)$, то k делится и на m, и на l, а значит, делится на n в силу взаимной простоты m и l. Отсюда следует, что гомоморфизм φ инъективен. Поскольку множества $\mathbb{Z}_n$ и $\mathbb{Z}_m \times \mathbb{Z}_l$ содержат одинаковое число элементов, отображение φ биективно. □

Следствие 6. *Пусть $n \geqslant 2$ — натуральное число и $n = p_1^{k_1} \ldots p_s^{k_s}$ — его разложение в произведение простых множителей (где $p_i \neq p_j$ при $i \neq j$). Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}.$$

Всюду в этой и следующей лекции $(A, +)$ — абелева группа с аддитивной формой записи операции. Для произвольного элемента $a \in A$ и целого числа s положим

$$sa = \begin{cases} \underbrace{a + \ldots + a}_{s}, & \text{если } s > 0; \\ 0, & \text{если } s = 0; \\ \underbrace{(-a) + \ldots + (-a)}_{|s|}, & \text{если } s < 0. \end{cases}$$

Определение 21. Абелева группа A называется *конечно порождённой*, если найдутся такие элементы $a_1, \ldots, a_n \in A$, что всякий элемент $a \in A$ представим в виде $a = s_1 a_1 + \ldots + s_n a_n$ для некоторых целых чисел $s_1, \ldots, s_n$. При этом элементы $a_1, \ldots, a_n$ называются *порождающими* или *образующими* группы A.

Замечание 5. Всякая конечно порождённая группа конечна или счётна.

Замечание 6. Всякая конечная группа является конечно порождённой.

Определение 22. Конечно порождённая абелева группа A называется *свободной*, если в ней существует *базис*, т. е. такой набор элементов $a_1, \ldots, a_n$, что каждый элемент $a \in A$ единственным образом представим в виде $a = s_1 a_1 + \ldots + s_n a_n$, где $s_1, \ldots, s_n \in \mathbb{Z}$. При этом число n называется *рангом* свободной абелевой группы A и обозначается $\operatorname{rk} A$.

Пример 3. Абелева группа $\mathbb{Z}^n := \{(c_1, \ldots, c_n) \mid c_i \in \mathbb{Z}\}$ является свободной с базисом

$$\begin{aligned} e_1 &= (1, 0, \ldots, 0), \\ e_2 &= (0, 1, \ldots, 0), \\ &\ldots \\ e_n &= (0, 0, \ldots, 1). \end{aligned}$$

Этот базис называется *стандартным*. В группе $\mathbb{Z}^n$ можно найти и много других базисов. Ниже мы все их опишем.

Предложение 5. *Ранг свободной абелевой группы определён корректно, т. е. любые два её базиса содержат одинаковое число элементов.*

Доказательство. Пусть $a_1, \ldots, a_n$ и $b_1, \ldots, b_m$ — два базиса группы A. Предположим, что $n < m$. Элементы $b_1, \ldots, b_m$ однозначно разлагаются по базису $a_1, \ldots, a_n$, поэтому мы можем записать

$$\begin{aligned} b_1 &= s_{11}a_1 + s_{12}a_2 + \ldots + s_{1n}a_n, \\ b_2 &= s_{21}a_1 + s_{22}a_2 + \ldots + s_{2n}a_n, \\ &\ldots \\ b_m &= s_{m1}a_1 + s_{m2}a_2 + \ldots + s_{mn}a_n, \end{aligned}$$

где все коэффициенты s_{ij} — целые числа. Рассмотрим прямоугольную матрицу $S = (s_{ij})$ размера $m \times n$. Так как $n < m$, то ранг этой матрицы не превосходит n, а значит, строки этой матрицы линейно зависимы над $\mathbb{Q}$. Домножая коэффициенты этой зависимости на наименьшее общее кратное их знаменателей, мы найдём такие целые $s_1, \ldots, s_m$, из которых не все равны нулю, что $s_1b_1 + \ldots + s_mb_m = 0$. Поскольку $0 = 0b_1 + \ldots + 0b_m$, это противоречит однозначной выразимости элемента 0 через базис $b_1, \ldots, b_m$. □

Предложение 6. *Всякая свободная абелева группа ранга n изоморфна группе $\mathbb{Z}^n$.*

Доказательство. Пусть A — свободная абелева группа, и пусть $a_1, \ldots, a_n$ — её базис. Рассмотрим отображение

$$\varphi\colon \mathbb{Z}^n \to A, \quad (s_1, \ldots, s_n) \mapsto s_1a_1 + \ldots + s_na_n.$$

Легко видеть, что φ — гомоморфизм. Так как всякий элемент $a \in A$ представим в виде $s_1a_1 + \ldots + s_na_n$, где $s_1, \ldots, s_n \in \mathbb{Z}$, то φ сюръективен. Из единственности такого представления следует инъективность φ. Значит, φ — изоморфизм. □

Пусть $e_1', \ldots, e_n'$ — некоторый набор элементов из $\mathbb{Z}^n$. Выразив эти элементы через стандартный базис $e_1, \ldots, e_n$, мы можем записать

$$(e_1', \ldots, e_n') = (e_1, \ldots, e_n)C,$$

где C — целочисленная квадратная матрица порядка n.

Предложение 7. *Элементы $e_1', \ldots, e_n'$ составляют базис группы $\mathbb{Z}^n$ тогда и только тогда, когда* $\det C = \pm 1$.

Доказательство. Предположим сначала, что $e_1', \ldots, e_n'$ — базис. Тогда элементы $e_1, \ldots, e_n$ через него выражаются, поэтому $(e_1, \ldots, e_n) = (e_1', \ldots, e_n')D$ для некоторой целочисленной квадратной матрицы D порядка n. Но тогда $(e_1, \ldots, e_n) = (e_1, \ldots, e_n)CD$, откуда $CD = E_n$, где E_n — единичная матрица порядка n. Значит, $(\det C)(\det D) = 1$. Учитывая, что $\det C$ и $\det D$ — целые числа, мы получаем $\det C = \pm 1$.

Обратно, пусть $\det C = \pm 1$. Тогда матрица C^{-1} является целочисленной, а соотношение $(e_1, \ldots, e_n) = (e_1', \ldots, e_n')C^{-1}$ показывает, что элементы $e_1, \ldots, e_n$ выражаются через $e_1', \ldots, e_n'$. Но $e_1, \ldots, e_n$ — базис, поэтому элементы $e_1', \ldots, e_n'$ порождают группу $\mathbb{Z}^n$. Осталось доказать, что всякий элемент из $\mathbb{Z}^n$ однозначно через них выражается. Предположим, что $s_1'e_1' + \ldots + s_n'e_n' = s_1''e_1' + \ldots + s_n''e_n'$ для некоторых целых чисел $s_1', \ldots, s_n', s_1'', \ldots, s_n''$. Мы можем это переписать в следующем виде:

$$(e_1', \ldots, e_n') \begin{pmatrix} s_1' \\ \vdots \\ s_n' \end{pmatrix} = (e_1', \ldots, e_n') \begin{pmatrix} s_1'' \\ \vdots \\ s_n'' \end{pmatrix}.$$

Учитывая, что $(e_1', \ldots, e_n') = (e_1, \ldots, e_n)C$ и что $e_1, \ldots, e_n$ — это базис, получаем

$$C \begin{pmatrix} s_1' \\ \vdots \\ s_n' \end{pmatrix} = C \begin{pmatrix} s_1'' \\ \vdots \\ s_n'' \end{pmatrix}.$$

Домножая это равенство слева на C^{-1}, окончательно получаем

$$\begin{pmatrix} s_1' \\ \vdots \\ s_n' \end{pmatrix} = \begin{pmatrix} s_1'' \\ \vdots \\ s_n'' \end{pmatrix}.$$

□

Теорема 2. *Всякая подгруппа N свободной абелевой группы L ранга n является свободной абелевой группой ранга $\leqslant n$.*

Доказательство. Воспользуемся индукцией по n. При $n = 0$ доказывать нечего. Пусть $n > 0$ и $e_1, \ldots, e_n$ — базис группы L. Рассмотрим в L подгруппу

$$L_1 = \langle e_1, \ldots, e_{n-1} \rangle := \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_{n-1}.$$

Это свободная абелева группа ранга $n - 1$. По предположению индукции подгруппа $N_1 := N \cap L_1 \subseteq L_1$ является свободной абелевой группой ранга $m \leqslant n - 1$. Зафиксируем в N_1 базис $f_1, \ldots, f_m$.

Рассмотрим отображение

$$\varphi\colon N \to \mathbb{Z}, \quad s_1e_1 + \ldots + s_ne_n \mapsto s_n.$$

Легко видеть, что φ — гомоморфизм и что $\operatorname{Ker}\varphi = N_1$. Далее, $\operatorname{Im}\varphi$ — подгруппа в $\mathbb{Z}$, по предложению 1 из лекции 1 она имеет вид $k\mathbb{Z}$ для некоторого целого $k \geqslant 0$. Если $k = 0$, то $N \subseteq L_1$, откуда $N = N_1$ и всё доказано. Если $k > 0$, то пусть f_{m+1} — какой-нибудь элемент из N, для которого $\varphi(f_{m+1}) = k$. Докажем, что $f_1, \ldots, f_m, f_{m+1}$ — базис в N. Пусть $f \in N$ — произвольный элемент, и пусть $\varphi(f) = sk$, где $s \in \mathbb{Z}$. Тогда $\varphi(f - sf_{m+1}) = 0$, откуда $f - sf_{m+1} \in N_1$ и, следовательно, $f - sf_{m+1} = s_1f_1 + \ldots + s_mf_m$ для некоторых $s_1, \ldots, s_m \in \mathbb{Z}$. Значит, $f = s_1f_1 + \ldots + s_mf_m + sf_{m+1}$ и элементы $f_1, \ldots, f_m, f_{m+1}$ порождают группу N. Осталось доказать, что они образуют базис в N. Предположим, что

$$s_1f_1 + \ldots + s_mf_m + s_{m+1}f_{m+1} = s'_1f_1 + \ldots + s'_mf_m + s'_{m+1}f_{m+1}$$

для некоторых целых чисел $s_1, \ldots, s_m, s_{m+1}, s'_1, \ldots, s'_m, s'_{m+1}$. Рассмотрев образ обеих частей этого равенства при гомоморфизме φ, получаем $s_{m+1}k = s'_{m+1}k$, откуда $s_{m+1} = s'_{m+1}$ и

$$s_1f_1 + \ldots + s_mf_m = s'_1f_1 + \ldots + s'_mf_m.$$

Но $f_1, \ldots, f_m$ — базис в N_1, поэтому $s_1 = s'_1, \ldots, s_m = s'_m$. $\square$

Лекция 4

Теорема о согласованных базисах. Алгоритм приведения целочисленной матрицы к диагональному виду. Строение конечно порождённых абелевых групп. Конечные абелевы группы.

В теории абелевых групп операция прямого произведения конечного числа групп обычно называется *прямой суммой* и обозначается символом $\oplus$, так что пишут $A_1 \oplus A_2 \oplus \ldots \oplus A_n$ вместо $A_1 \times A_2 \times \ldots \times A_n$.

Дадим более точное описание подгрупп свободных абелевых групп.

Теорема о согласованных базисах. Для всякой подгруппы N свободной абелевой группы L ранга n найдётся такой базис $e_1, \ldots, e_n$ группы L и такие натуральные числа $u_1, \ldots, u_m$, $m \leqslant n$, что $u_1 e_1, \ldots, u_m e_m$ — базис группы N и $u_i | u_{i+1}$ при $i = 1, \ldots, m-1$.

Замечание 7. Числа $u_1, \ldots, u_p$, фигурирующие в теореме о согласованных базисах, называются *инвариантными множителями* подгруппы $N \subseteq L$. Можно показать, что они определены по подгруппе однозначно.

Следствие 7. *В условиях теоремы о согласованных базисах имеет место изоморфизм*

$$L/N \cong \mathbb{Z}_{u_1} \times \ldots \times \mathbb{Z}_{u_m} \times \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n-m}.$$

Доказательство. Рассмотрим изоморфизм $L \cong \mathbb{Z}^n = \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n}$, сопоставляющий произвольному элементу $s_1 e_1 + \ldots + s_n e_n \in L$ набор $(s_1, \ldots, s_n) \in \mathbb{Z}^n$. При этом изоморфизме подгруппа $N \subseteq L$ отождествляется с подгруппой

$$u_1\mathbb{Z} \times \ldots \times u_m\mathbb{Z} \times \underbrace{\{0\} \times \ldots \times \{0\}}_{n-m} \subseteq \mathbb{Z}^n.$$

Теперь требуемый результат получается применением теоремы о факторизации по сомножителям. $\square$

Теперь вернемся к доказательству теоремы о согласованных базисов. Однако это требует некоторой подготовки.

Определение 23. *Целочисленными элементарными преобразованиями строк* матрицы называются преобразования следующих трёх типов:

1) прибавление к одной строке другой, умноженной на целое число;

2) перестановка двух строк;

3) умножение одной строки на -1.

Аналогично определяются *целочисленные элементарные преобразования столбцов* матрицы.

Прямоугольную матрицу $C = (c_{ij})$ размера $n \times m$ назовём *диагональной* и обозначим $\mathrm{diag}(u_1, \ldots, u_p)$, если $c_{ij} = 0$ при $i \neq j$ и $c_{ii} = u_i$ при $i = 1, \ldots, p$, где $p = \min(n, m)$.

Предложение 8. *Всякую прямоугольную целочисленную матрицу $C = (c_{ij})$ с помощью элементарных преобразований строк и столбцов можно привести к виду $diag(u_1, \ldots, u_p)$, где $u_1, \ldots, u_p \geqslant 0$ и $u_i | u_{i+1}$ при $i = 1, \ldots, p-1$.*

Доказательство. Если $C = 0$, то доказывать нечего. Если $C \neq 0$, но $c_{11} = 0$, то переставим строки и столбцы и получим $c_{11} \neq 0$. Умножив, если нужно, первую строку на -1, добьёмся условия $c_{11} > 0$. Теперь будем стремиться уменьшить c_{11}.

Если какой-то элемент c_{i1} не делится на c_{11}, то разделим с остатком: $c_{i1} = qc_{11} + r$. Вычитая из i-й строки 1-ю строку, умноженную на q, и затем переставляя 1-ю и i-ю строки, уменьшаем c_{11}. Повторяя эту процедуру, в итоге добиваемся, что все элементы 1-й строки и 1-го столбца делятся на c_{11}.

Если какой-то c_{ij} не делится на c_{11}, то поступаем следующим образом. Вычтя из i-й строки 1-ю строку с подходящим коэффициентом, добьёмся $c_{i1} = 0$. После этого прибавим к 1-й строке i-ю строку. При этом c_{11} не изменится, а c_{1j} перестанет делиться на c_{11}, и мы вновь сможем уменьшить c_{11}.

В итоге добьёмся того, что все элементы делятся на c_{11}. После этого обнулим все элементы 1-й строки и 1-го столбца, начиная со вторых, и продолжим процесс с меньшей матрицей. $\square$

Теперь мы готовы доказать теорему о согласованных базисах.

Доказательство теоремы о согласованных базисах. Мы знаем, что N является свободной абелевой группой ранга $m \leqslant n$. Пусть $e_1, \ldots, e_n$ — базис в L и $f_1, \ldots, f_m$ — базис в N. Тогда $(f_1, \ldots, f_m) = (e_1, \ldots, e_n)C$, где C — целочисленная матрица размера $n \times m$ и ранга m. Покажем, что целочисленные элементарные преобразования строк (столбцов) матрицы C — это в точности элементарные преобразования над базисом в L (в N). Для этого рассмотрим сначала случай строк. Заметим, что каждое из целочисленных элементарных преобразований строк реализуется при помощи умножения матрицы C слева на квадратную матрицу P порядка n, определяемую следующим образом:

(1) в случае прибавления к i-й строке j-й, умноженной на целое число z, в матрице P на диагонали стоят единицы, на (ij)-м месте — число z, а на остальных местах — нули;

(2) в случае перестановки i-й и j-й строк имеем $p_{ij} = p_{ji} = 1$, $p_{kk} = 1$ при $k \neq i, j$, а на остальных местах стоят нули;

(3) в случае умножения i-й строки на -1 имеем $p_{ii} = -1$, $p_{jj} = 1$ при $j \neq i$, а на остальных местах стоят нули.

Теперь заметим, что равенство $(f_1, \ldots, f_m) = (e_1, \ldots, e_n)C$ эквивалентно равенству $(f_1, \ldots, f_m) = (e_1, \ldots, e_n)P^{-1}PC$. Таким образом, базис $(f_1, \ldots, f_m)$ выражается через новый базис $(e'_1, \ldots, e'_n) := (e_1, \ldots, e_n)P^{-1}$ при помощи матрицы PC.

В случае столбцов всё аналогично: каждое из целочисленых элементарных преобразований столбцов реализуется при помощи умножения матрицы C справа на некоторую квадратную матрицу Q порядка m (определяемую почти так же, как P). В этом случае имеем $(f_1, \ldots, f_m)Q = (e_1, \ldots, e_n)CQ$, так что новый базис $(f'_1, \ldots, f'_m) := (f_1, \ldots, f_m)Q$ выражается через $(e_1, \ldots, e_n)$ при помощи матрицы CQ.

Воспользовавшись предложением 8, мы можем привести матрицу C при помощи целочисленных элементарных преобразований строк и столбцов к диагональному виду $C'' = \mathrm{diag}(u_1, \ldots, u_m)$, где $u_i | u_{i+1}$ для всех $i = 1, \ldots, m-1$. С учётом сказанного выше это означает, что для некоторого базиса $e''_1, \ldots, e''_n$ в L и некоторого базиса $f''_1, \ldots, f''_m$ в N справедливо соотношение $(f''_1, \ldots, f''_m) = (e''_1, \ldots, e''_n)C''$. Иными словами, $f''_i = u_i e''_i$ для всех $i = 1, \ldots, m$, а это и требовалось. □

Определение 24. Конечная абелева группа A называется *примарной*, если её порядок равен p^k для некоторого простого числа p.

Замечание 8. В общем случае (когда группы не предполагаются коммутативными) конечная группа G с условием $|G| = p^k$ (p — простое) называется *p-группой.*

Следствие 1 лекции 3 показывает, что каждая конечная циклическая группа разлагается в прямую сумму примарных циклических подгрупп.

Теорема 3. *Всякая конечно порождённая абелева группа A разлагается в прямую сумму примарных и бесконечных циклических подгрупп, т. е.*

$$A \cong \mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}, \qquad (1)$$

где $p_1, \ldots, p_s$ — простые числа (не обязательно попарно различные) и $k_1, \ldots, k_s \in \mathbb{N}$. Кроме того, число бесконечных циклических слагаемых, а также число и порядки примарных циклических слагаемых определено однозначно.

Сразу выделим некоторые следствия из этой теоремы.

Следствие 8. *Абелева группа A является конечно порождённой тогда и только тогда, когда A разлагается в прямую сумму циклических подгрупп.*

Доказательство. В одну сторону следует из теоремы. В другую сторону: пусть $A = A_1 \oplus \ldots \oplus A_m$, где A_i — циклическая подгруппа, то есть $A_i = \langle a_i \rangle$, $a_i \in A$. Тогда $\{a_1, \ldots, a_m\}$ — набор порождающих элементов для группы A. □

Следствие 9. *Всякая конечная абелева группа разлагается в прямую сумму примарных циклических подгрупп, причём число и порядки примарных циклических слагаемых определено однозначно.*

Теперь преступим к доказательству самой теоремы.

Доказательство. Пусть $a_1, \ldots, a_n$ — конечная система порождающих группы A. Рассмотрим гомоморфизм

$$\varphi\colon \mathbb{Z}^n \to A, \quad (s_1, \ldots, s_n) \mapsto s_1 a_1 + \ldots + s_n a_n.$$

Ясно, что φ сюръективен. Тогда по теореме о гомоморфизме получаем $A \cong \mathbb{Z}^n/N$, где $N = \operatorname{Ker}\varphi$. По теореме о согласованных базисах существует такой базис $e_1, \ldots, e_n$ группы $\mathbb{Z}^n$ и такие натуральные числа $u_1, \ldots, u_m$, $m \leqslant n$, что $u_1e_1, \ldots, u_me_m$ — базис группы N. Тогда имеем

$$\begin{array}{ccccccccccccc} L & = & \langle e_1\rangle & \oplus & \ldots & \oplus & \langle e_m\rangle & \oplus & \langle e_{m+1}\rangle & \oplus & \ldots & \oplus & \langle e_n\rangle, \\ N & = & \langle u_1e_1\rangle & \oplus & \ldots & \oplus & \langle u_me_m\rangle & \oplus & \{0\} & \oplus & \ldots & \oplus & \{0\}. \end{array}$$

Применяя теорему о факторизации по сомножителям, мы получаем

$$\mathbb{Z}^n/N \cong \mathbb{Z}/u_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/u_m\mathbb{Z} \oplus \underbrace{\mathbb{Z}/\{0\} \oplus \ldots \oplus \mathbb{Z}/\{0\}}_{n-m} \cong \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m} \oplus \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n-m}.$$

Чтобы добиться разложения (11), остаётся представить каждое из циклических слагаемых $\mathbb{Z}_{u_i}$ в виде прямой суммы примарных циклических подгрупп, воспользовавшись следствием 1 из лекции 3.

Перейдём к доказательству единственности разложения (11). Пусть $\langle c\rangle_q$ обозначает циклическую группу порядка q с порождающей c. Пусть имеется разложение

(2) $$A = \langle c_1\rangle_{p_1^{k_1}} \oplus \ldots \oplus \langle c_s\rangle_{p_s^{k_s}} \oplus \langle c_{s+1}\rangle_\infty \oplus \ldots \oplus \langle c_{s+t}\rangle_\infty$$

(заметьте, что мы просто переписали в другом виде правую часть соотношения (11)). Рассмотрим в A так называемую *подгруппу кручения*

$$\operatorname{Tor} A := \{a \in A \mid ma = 0 \text{ для некоторого } m \in \mathbb{N}\}.$$

Иными словами, $\operatorname{Tor} A$ — это подгруппа в A, состоящая из всех элементов конечного порядка. Выделим эту подгруппу в разложении (2). Рассмотрим произвольный элемент $a \in A$. Он представим в виде

$$a = r_1c_1 + \ldots + r_mc_m + r_{m+1}c_{m+1} + \ldots + r_nc_n$$

для некоторых целых чисел $r_1, \ldots, r_n$. Легко видеть, что a имеет конечный порядок тогда и только тогда, когда $r_{m+1} = \ldots = r_m = 0$. Отсюда получаем, что

(3) $$\operatorname{Tor} A = \langle c_1\rangle_{p_1^{k_1}} \oplus \ldots \oplus \langle c_s\rangle_{p_s^{k_s}}.$$

Применяя опять теорему о факторизации по сомножителям, мы получаем $A/\operatorname{Tor} A \cong \mathbb{Z}^t$, где t — количество бесконечных циклических подгрупп в разложении (11). Отсюда следует, что число t однозначно выражается в терминах самой группы A (как ранг свободной абелевой группы $A/\operatorname{Tor} A$). Значит, t не зависит от разложения (2).

Однозначность числа и порядков примарных циклических групп будет доказана на следующей лекции.

□

Лекция 5

Строение конечно порождённых абелевых груп (продолжение). Экспонента конечной абелевой группы. Действие группы на множестве. Орбиты и стабилизаторы.

Продолжим доказательство теоремы с прошлой лекции.

Теорема 4. *Всякая конечно порождённая абелева группа A разлагается в прямую сумму примарных и бесконечных циклических подгрупп, т. е.*

$$A \cong \mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_s}} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}, \tag{4}$$

где $p_1, \ldots, p_s$ — простые числа (не обязательно попарно различные) и $k_1, \ldots, k_s \in \mathbb{N}$. Кроме того, число бесконечных циклических слагаемых, а также число и порядки примарных циклических слагаемых определено однозначно.

Доказательство. На прошлой лекции мы доказали существование разложения и то, что количество бесконечных циклических групп $\mathbb{Z}$ определено однозначно. Для этого мы вводили понятие *подгруппы кручения*:

$$\operatorname{Tor} A = \langle c_1 \rangle_{p_1^{k_1}} \oplus \ldots \oplus \langle c_s \rangle_{p_s^{k_s}}. \tag{5}$$

Далее, для каждого простого числа p определим в A *подгруппу p-кручения*

$$\operatorname{Tor}_p A := \{a \in A \mid p^k a = 0 \text{ для некоторого } k \in \mathbb{N}\}. \tag{6}$$

Ясно, что $\operatorname{Tor}_p A \subset \operatorname{Tor} A$. Выделим подгруппу $\operatorname{Tor}_p A$ в разложении (5). Легко видеть, что $\langle c_i \rangle_{p_i^{k_i}} \subseteq \operatorname{Tor}_p A$ для всех i с условием $p_i = p$. Если же $p_i \neq p$, то по следствию 2 из теоремы Лагранжа (см. лекцию 2) порядок любого ненулевого элемента $x \in \langle c_i \rangle_{p_i^{k_i}}$ является степенью числа p_i, а значит, $p^k x \neq 0$ для всех $k \in \mathbb{N}$. Отсюда следует, что $\operatorname{Tor}_p A$ является суммой тех конечных слагаемых в разложении (5), порядки которых суть степени p. Поэтому доказательство теперь сводится к случаю, когда A — примарная группа.

Пусть $|A| = p^k$ и

$$A = \langle c_1 \rangle_{p^{k_1}} \oplus \ldots \oplus \langle c_r \rangle_{p^{k_r}}, \quad k_1 + \ldots + k_r = k.$$

Докажем индукцией по k, что набор чисел $k_1, \ldots, k_r$ не зависит от разложения.

Если $k = 1$, то $|A| = p$, но тогда $A \cong \mathbb{Z}_p$ по следствию 5 из теоремы Лагранжа (см. лекцию 2). Пусть теперь $k > 1$. Рассмотрим подгруппу $pA := \{pa \mid a \in A\}$. В терминах равенства (6) имеем

$$pA = \langle pc_1 \rangle_{p^{k_1 - 1}} \oplus \ldots \oplus \langle pc_r \rangle_{p^{k_r - 1}}.$$

В частности, при $k_i = 1$ соответствующее слагаемое равно $\{0\}$ (и тем самым исчезает). Так как $|pA| = p^{k-r} < p^k$, то по предположению индукции группа pA разлагается в прямую сумму примарных циклических подгрупп однозначно с точностью до порядка слагаемых. Следовательно, ненулевые числа в наборе $k_1 - 1, \ldots, k_r - 1$ определены однозначно (с точностью до перестановки). Отсюда мы находим значения k_i, отличные от 1. Количество тех k_i, которые равны 1, однозначно восстанавливается из условия $k_1 + \ldots + k_r = k$. $\square$

Заметим, что теорема о согласованных базисах даёт нам другое разложение конечной абелевой группы A:

$$A = \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}, \quad \text{где } u_i | u_{i+1} \text{ при } i = 1, \ldots, m-1. \tag{7}$$

Числа $u_1, \ldots, u_m$ называют *инвариантными множителями* конечной абелевой группы A.

Определение 25. *Экспонентой* конечной абелевой группы A называется число $\exp A$, равное наименьшему общему кратному порядков элементов из A. Легко заметить, что это равносильно следующему условию:

$$\exp A = \min\{n \in \mathbb{N} \mid na = 0 \text{ для всех } a \in A\}$$

Предложение 9. *Экспонента конечной абелевой группы A равна её последнему инвариантному множителю u_m.*

Доказательство. Обратимся к разложению (7). Так как $u_i | u_m$ для всех $i = 1, \ldots, m$, то $u_m a = 0$ для всех $a \in A$. Это означает, что $\exp A \leqslant u_m$ (и тем самым $\exp A \,|u_m$). С другой стороны, в A имеется циклическая подгруппа порядка u_m. Значит, $\exp A \geqslant u_m$. $\square$

Следствие 10. *Конечная абелева группа A является циклической тогда и только тогда, когда $\exp A = |A|$.*

Доказательство. Группа A является циклической тогда и только тогда, когда в разложении (7) присутствует только одно слагаемое, т. е. $A = \mathbb{Z}_{u_m}$ и $|A| = u_m$. $\square$

Пусть G — произвольная группа и X — некоторое множество.

Определение 26. *Действием* группы G на множестве X называется отображение $G \times X \to X$, $(g, x) \mapsto gx$, удовлетворяющее следующим условиям:

1) $ex = x$ для любого $x \in X$ (e — нейтральный элемент группы G);

2) $g(hx) = (gh)x$ для всех $g, h \in G$ и $x \in X$.

Обозначение: $G : X$.

Если задано действие группы G на множестве X, то каждый элемент $g \in G$ определяет биекцию $a_g \colon X \to X$ по правилу $a_g(x) = gx$ (обратным отображением для a_g будет $a_{g^{-1}}$). Обозначим через $S(X)$ группу всех биекций (перестановок) множества X с операцией композиции. Тогда отображение $a \colon G \to S(X)$, $g \mapsto a_g$, является гомоморфизмом групп. Действительно, для произвольных элементов $g, h \in G$ и $x \in X$ имеем

$$a_{gh}(x) = (gh)x = g(hx) = ga_h(x) = a_g(a_h(x)) = (a_g a_h)(x).$$

Можно показать, что задание действия группы G на множестве X равносильно заданию соответствующего гомоморфизма $a \colon G \to S(X)$.

Пример 4. Симметрическая группа S_n естественно действует на множестве $X = \{1, 2, \ldots, n\}$ по формуле $\sigma x = \sigma(x)$ ($\sigma \in S_n$, $x \in X$). Условие 1) здесь выполнено по определению тождественной подстановки, условие 2) выполнено по определению композиции подстановок.

Пусть задано действие группы G на множестве X.

Определение 27. *Орбитой* точки $x \in X$ называется подмножество

$$Gx = \{x' \in X \mid x' = gx \text{ для некоторого } g \in G\} = \{gx \mid g \in G\}.$$

Замечание 9. Для точек $x, x' \in X$ отношение «x' лежит в орбите Gx» является отношением эквивалентности:

(1) (рефлексивность) $x \in Gx$ для всех $x \in X$: это верно, так как $x = ex \in Gx$ для всех $x \in X$;

(2) (симметричность) если $x' \in Gx$, то $x \in Gx'$: это верно, так как из условия $x' = gx$ следует $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x' \in Gx'$;

(3) (транзитивность) если $x' \in Gx$ и $x'' \in Gx'$, то $x'' \in Gx$: это верно, так как из условий $x' = gx$ и $x'' = hx'$ следует $x'' = hx' = h(gx) = (hg)x \in Gx$.

Отсюда вытекает, что множество X разбивается в объединение попарно непересекающихся орбит действия группы G.

Определение 28. *Стабилизатором* (*стационарной подгруппой*) точки $x \in X$ называется подгруппа $\mathrm{St}(x) := \{g \in G \mid gx = x\}$.

Упражнение 1. Проверьте, что множество $\mathrm{St}(x)$ действительно является подгруппой в G.

Лемма 5. *Пусть конечная группа G действует на множестве X. Тогда для всякого элемента $x \in X$ справедливо равенство*

$$|Gx| = |G|/|\mathrm{St}(x)|.$$

В частности, число элементов в (любой) орбите делит порядок группы G.

Доказательство. Рассмотрим множество[1] $G/\mathrm{St}(x)$ левых смежных классов группы G по подгруппе $\mathrm{St}(x)$ и определим отображение $\psi \colon G/\mathrm{St}(x) \to Gx$ по формуле $g\mathrm{St}(x) \mapsto gx$. Это определение корректно, поскольку для любого другого представителя g' левого смежного класса $g\mathrm{St}(x)$ имеем $g' = gh$, где $h \in \mathrm{St}(x)$, и тогда $g'x = (gh)x = g(hx) = gx$. Сюръективность отображения ψ следует из определения орбиты Gx. Проверим инъективность. Предположим, что $g_1\mathrm{St}(x) = g_2\mathrm{St}(x)$ для некоторых $g_1, g_2 \in G$. Тогда $g_1x = g_2x$. Подействовав на левую и правую части элементом g_2^{-1}, получим $(g_2^{-1}g_1)x = x$, откуда $g_2^{-1}g_1 \in \mathrm{St}(x)$. Последнее и означает, что $g_1\mathrm{St}(x) = g_2\mathrm{St}(x)$. Итак, мы показали, что отображние ψ является биекцией. Значит, $|Gx| = |G/\mathrm{St}(x)| = [G : \mathrm{St}(x)]$ и требуемое равенство вытекает из теоремы Лагранжа (см. лекцию 1). $\square$

[1]Это множество может не быть факторгруппой, так как подгруппа $\mathrm{St}(x)$ не обязана быть нормальной в G.

Пример 5. Рассмотрим действие группы $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ на множестве $\mathbb{C}$, заданное формулой $(z, w) \mapsto zw$, где $z \in S^1$, $w \in \mathbb{C}$, а zw — обычное произведение комплексных чисел. Для этого действия орбитами будут множества вида $|z| = c$, где $c \in \mathbb{R}_{\geqslant 0}$, — это всевозможные окружности с центром в нуле, а также отдельная орбита, состоящая из нуля. Имеем

$$\mathrm{St}(z) = \begin{cases} \{1\}, & \text{если } z \neq 0; \\ S^1, & \text{если } z = 0. \end{cases}$$

Лекция 6

Три действия группы на себе. Теорема Кэли. Классы сопряжённости. Кольца. Делители нуля, обратимые элементы, нильпотенты. Поля и алгебры. Идеалы.

Пусть G — произвольная группа. Рассмотрим три действия G на самой себе, т. е. положим $X = G$:

1) действие *умножениями слева (левыми сдвигами)*: $(g, h) \mapsto gh$;

2) действие *умножениями справа (правыми сдвигами)*: $(g, h) \mapsto hg^{-1}$;

3) действие *сопряжениями*: $(g, h) \mapsto ghg^{-1}$.

Замечание 10. Для действий левыми и правыми сдвигами есть ровно одна орбита (сама G) и стабилизатор любой точки тривиален, то есть $\mathrm{St}(x) = \{0\}$.

Определение 29. Орбитой действия сопряжениями называются *классами сопряженности*

Пример 6. В любой группе G есть класс сопряженности $\{e\}$.
Также, если G коммутативна, то $\{x\}$ является классом сопряженности для всех x из G.

Теорема Кэли. Всякая конечная группа G порядка n изоморфна подгруппе симметрической группы S_n.

Доказательство. Рассмотрим действие группы G на себе левыми сдвигами. Как мы знаем, это действие свободно, поэтому соответствующий гомоморфизм $a\colon G \to S(G) \simeq S_n$ инъективен, т. е. $\operatorname{Ker} a = \{e\}$. Учитывая, что $G/\{e\} \cong G$, по теореме о гомоморфизме получаем $G \cong \operatorname{Im} a$. □

Теперь приступим к изучению колец.

Определение 30. *Кольцом* называется множество R с двумя бинарными операциями «$+$» (сложение) и «$\times$» (умножение), обладающими следующими свойствами:

1) $(R, +)$ является абелевой группой (называемой *аддитивной группой* кольца R);

2) выполнены *левая и правая дистрибутивности*, т.е.

$$a(b + c) = ab + ac \quad \text{и} \quad (b + c)a = ba + ca \quad \text{для всех } a, b, c \in R.$$

В этом курсе мы рассматриваем только ассоциативные кольца с единицей, поэтому дополнительно считаем, что выполнены ещё два свойства:

3) $a(bc) = (ab)c$ для всех $a, b, c \in R$ (*ассоциативность умножения*);

4) существует такой элемент $1 \in R$ (называемый *единицей*), что

$$a1 = 1a = a \text{ для всякого } a \in R. \tag{8}$$

Замечание 11. В произвольном кольце R выполнены равенства

$$a0 = 0a = 0 \text{ для всякого } a \in R. \tag{9}$$

В самом деле, имеем $a0 = a(0+0) = a0+a0$, откуда $0 = a0$. Аналогично устанавливается равенство $0a = 0$.

Замечание 12. Если кольцо R содержит более одного элемента, то $0 \neq 1$. Это следует из соотношений (8) и (9).

Примеры колец:

(1) числовые кольца $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;
(2) кольцо $\mathbb{Z}_n$ вычетов по модулю n;
(3) кольцо $\mathrm{Mat}(n \times n, \mathbb{R})$ матриц с коэффициентами из $\mathbb{R}$;
(4) кольцо $\mathbb{R}[x]$ многочленов от переменной x с коэффициентами из $\mathbb{R}$;
(5) кольцо $\mathbb{R}[[x]]$ *формальных степенных рядов* от переменной x с коэффициентами из $\mathbb{R}$:

$$\mathbb{R}[[x]] := \{\sum_{i=0}^{\infty} a_i x^i \mid a_i \in \mathbb{R}\};$$

(6) кольцо $\mathcal{F}(M, \mathbb{R})$ всех функций из множества M во множество $\mathbb{R}$ с операциями поточечного сложения и умножения:

$$(f_1 + f_2)(m) := f_1(m) + f_2(m); \quad (f_1 f_2)(m) := f_1(m) f_2(m) \quad \text{для всех} \quad f_1, f_2 \in \mathcal{F}(M, \mathbb{R}), m \in M.$$

Замечание 13. В примерах (3)–(6) вместо $\mathbb{R}$ можно брать любое кольцо, в частности $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_n$.

Замечание 14. Обобщая пример (4), можно рассматривать кольцо $\mathbb{R}[x_1,\ldots,x_n]$ многочленов от нескольких переменных $x_1,\ldots,x_n$ с коэффициентами из $\mathbb{R}$.

Определение 31. Кольцо R называется *коммутативным*, если $ab = ba$ для всех $a, b \in R$.

Все перечисленные в примерах (1)–(6) кольца, кроме $\mathrm{Mat}(n\times n,\mathbb{R})$ при $n \geqslant 2$, коммутативны.

Пусть R — кольцо.

Определение 32. Элемент $a \in R$ называется *обратимым*, если найдётся такой $b \in R$, что $ab = ba = 1$. Такой элемент b обозначается классическим образом как a^{-1}.

Замечание 15. Все обратимые элементы кольца R образуют группу относительно операции умножения.

Определение 33. Элемент $a \in R$ называется *левым* (соответственно *правым*) *делителем нуля*, если $a \neq 0$ и найдётся такой $b \in R$, $b \neq 0$, что $ab = 0$ (соответственно $ba = 0$).

Замечание 16. В случае коммутативных колец понятия левого и правого делителей нуля совпадают, поэтому говорят просто о делителях нуля.

Замечание 17. Все делители нуля в R необратимы: если $ab = 0$, $a \neq 0$, $b \neq 0$ и существует a^{-1}, то получаем $a^{-1}ab = a^{-1}0$, откуда $b = 0$ — противоречие.

Определение 34. Элемент $a \in R$ называется *нильпотентом*, если $a \neq 0$ и найдётся такое $m \in \mathbb{N}$, что $a^m = 0$.

Замечание 18. Всякий нильпотент в R является делителем нуля: если $a \neq 0$, $a^m = 0$ и число m наименьшее с таким свойством, то $m \geqslant 2$ и $a^{m-1} \neq 0$, откуда $aa^{m-1} = a^{m-1}a = 0$.

Определение 35. *Полем* называется коммутативное ассоциативное кольцо K с единицей, в котором всякий ненулевой элемент обратим.

Замечание 19. Тривиальное кольцо $\{0\}$ полем не считается, поэтому $0 \neq 1$ в любом поле.

Примеры полей: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$.

Предложение 10. *Кольцо вычетов $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое число.*

Доказательство. Если число n составное, то $n = mk$, где $1 < m, k < n$. Тогда $\overline{m}\overline{k} = \overline{n} = \overline{0}$. Следовательно, $\overline{k}$ и $\overline{m}$ — делители нуля в $\mathbb{Z}_n$, ввиду чего не все ненулевые элементы там обратимы.

Если $n = p$ — простое число, то возьмём произвольный ненулевой вычет $\overline{a} \in \mathbb{Z}_p$ и покажем, что он обратим. Рассмотрим вычеты

$$\overline{1}\overline{a}, \overline{2}\overline{a}, \ldots, \overline{(p-1)}\overline{a}. \tag{10}$$

Если $\overline{ra} = \overline{sa}$ при $1 \leqslant r, s \leqslant p-1$, то число $(r-s)a$ делится на p. В силу взаимной простоты чисел a и p получаем, что число $r - s$ делится на p. Тогда из условия $|r-s| \leqslant p-2$ следует, что $r = s$. Это рассуждение показывает, что все вычеты (10) попарно различны. Поскольку все они отличны от нуля, среди них должна найтись единица: существует такое $b \in \{1,\ldots,p-1\}$, что $\overline{b}\overline{a} = \overline{1}$. Это и означает, что вычет $\overline{a}$ обратим. □

Определение 36. *Алгеброй* над полем K (или кратко K*-алгеброй*) называется множество A с операциями сложения, умножения и умножения на элементы поля K, обладающими следующими свойствами:

1) относительно сложения и умножения A есть кольцо;

2) относительно сложения и умножения на элементы из K множество A есть векторное пространство;

3 $(\lambda a)b = a(\lambda b) = \lambda(ab)$ для любых $\lambda \in K$ и $a, b \in A$.

Размерностью алгебры A называется её размерность как векторного пространства над K. (Обозначение: $\dim_K A$.)

Примеры.

1) Алгебра матриц $\mathrm{Mat}(n\times n, K)$ над произвольным полем K. Её размерность равна n^2.

2) Алгебра $K[x]$ многочленов от переменной x над произвольным полем K. Её размерность равна ∞.

3) K, F — поля, $K \subset F$, F — алгебра над K.
Если это $\mathbb{R} \subset \mathbb{C}$, то $\dim_{\mathbb{R}} \mathbb{C} = 2$.
Если это $\mathbb{Q} \subset \mathbb{R}$, то $\dim_{\mathbb{Q}} \mathbb{R} = \infty$.

Определение 37. *Подкольцом* кольца R называется всякое подмножество $R' \subseteq R$, замкнутое относительно операций сложения и умножения (т. е. $a+b \in R'$ и $ab \in R'$ для всех $a, b \in R'$) и являющееся кольцом относительно этих операций. *Подполем* называется всякое подкольцо, являющееся полем.

Например, $\mathbb{Z}$ является подкольцом в $\mathbb{Q}$, а скалярные матрицы образуют подполе в кольце $\mathrm{Mat}(n \times n, \mathbb{R})$.

Замечание 20. Если K — подполе поля F, то F является алгеброй над K. Так, поле $\mathbb{C}$ является бесконечномерной алгеброй над $\mathbb{Q}$, тогда как над $\mathbb{R}$ имеет размерность 2.

Определение 38. *Подалгеброй* алгебры A (над полем K) называется всякое подмножество $A' \subseteq A$, замкнутое относительно всех трёх имеющихся в A операций (сложения, умножения и умножения на элементы из K) и являющееся алгеброй (над K) относительно этих операций.

Легко видеть, что подмножество $A' \subseteq A$ является алгеброй тогда и только тогда, когда оно является одновременно подкольцом и векторным подпространством в A.

Гомоморфизмы колец, алгебр определяются естественным образом как отображения, сохраняющие все операции.

Упражнение 2. Сформулируйте точные определения гомоморфизма колец и гомоморфизма алгебр.

Определение 39. *Изоморфизмом* колец, алгебр называется всякий гомоморфизм, являющийся биекцией.

В теории групп нормальные подгруппы обладают тем свойством, что по ним можно «факторизовать». В этом смысле аналогами нормальных подгрупп в теории колец служат идеалы.

Определение 40. Подмножество I кольца R называется (*двусторонним*) *идеалом*, если оно является подгруппой по сложению и $ra \in I$, $ar \in I$ для любых $a \in I$, $r \in R$.

Замечание 21. В некоммутативных кольцах рассматривают также левые и правые идеалы.

В каждом кольце R есть *несобственные* идеалы $I = 0$ и $I = R$. Все остальные идеалы называются *собственными*.

Упражнение 3. Пусть R — коммутативное кольцо. С каждым элементом $a \in R$ связан идеал $(a) := \{ra \mid r \in R\}$.

Определение 41. Идеал I называется *главным*, если существует такой элемент $a \in R$, что $I = (a)$. (В этой ситуации говорят, что I порождён элементом a.)

Пример. В кольце $\mathbb{Z}$ подмножество $k\mathbb{Z}$ ($k \in \mathbb{Z}$) является главным идеалом, порождённым элементом k. Более того, все идеалы в $\mathbb{Z}$ являются главными.

Замечание 22. Главный идеал (a) является несобственным тогда и только тогда, когда $a = 0$ или a обратим.

Более общо, с каждым подмножеством $S \subseteq R$ связан идеал

$$(S) := \{r_1 a_1 + \ldots + r_k a_k \mid a_i \in S, r_i \in R, k \in \mathbb{N}\}.$$

(Проверьте, что это действительно идеал!) Это наименьший по включению идеал в R, содержащий подмножество S. В этой ситуации говорят, что идеал $I = (S)$ порождён подмножеством S.

Лекция 7

Факторкольца. Теорема о гомоморфизме колец. Евклидовы кольца, кольца главных идеалов и факториальные кольца.

Вернёмся к случаю произвольного кольца R. Поскольку любой идеал I является подгруппой абелевой группы $(R,+)$, мы можем рассмотреть факторгруппу R/I. Введём на ней умножение по формуле

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

Покажем, что это определение корректно. Пусть элементы $a', b' \in R$ таковы, что $a'+I = a+I$ и $b'+I = b+I$. Проверим, что $a'b'+I = ab+I$. Заметим, что $a' = a+x$ и $b' = b+y$ для некоторых $x, y \in I$. Тогда

$$a'b'+I = (a+x)(b+y)+I = ab+ay+xb+xy+I = ab+I,$$

поскольку $ay, xb, xy \in I$ в силу определения идеала.

Упражнение 4. Проверьте, что множество R/I является кольцом относительно имеющейся там операции сложения и только что введённой операции умножения.

Определение 42. Кольцо R/I называется *факторкольцом* кольца R по идеалу I.

Пример. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Пусть $\varphi\colon R \to R'$ — гомоморфизм колец. Тогда определены его ядро $\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\}$ и образ $\operatorname{Im}\varphi = \{\varphi(r) \mid r \in R\} \subseteq R'$.

Лемма 6. *Ядро* $\operatorname{Ker}\varphi$ *является идеалом в* R.

Доказательство. Так как φ — гомоморфизм абелевых групп, то $\operatorname{Ker}\varphi$ является подгруппой в R по сложению. Покажем теперь, что $ra \in \operatorname{Ker}\varphi$ и $ar \in \operatorname{Ker}\varphi$ для произвольных элементов $a \in \operatorname{Ker}\varphi$ и $r \in R$. Имеем $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$, откуда $ra \in \operatorname{Ker}\varphi$. Аналогично получаем $ar \in \operatorname{Ker}\varphi$. □

Упражнение 5. Проверьте, $\operatorname{Im}\varphi$ — подкольцо в R'.

Теорема о гомоморфизме для колец. Пусть $\varphi\colon R \to R'$ – гомоморфизм колец. Тогда имеет место изоморфизм

$$R/\operatorname{Ker}\,\varphi \cong \operatorname{Im}\varphi.$$

Доказательство. Положим для краткости $I = \operatorname{Ker}\varphi$ и рассмотрим отображение

$$\pi\colon R/I \to \operatorname{Im}\varphi, \quad a+I \mapsto \varphi(a).$$

Из доказательства теоремы о гомоморфизме для групп следует, что отображение π корректно определено и является изоморфизмом абелевых групп (по сложению). Покажем, что π — изоморфизм колец. Для этого остаётся проверить, что π сохраняет операцию умножения:

$$\pi((a+I)(b+I)) = \pi(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \pi(a+I)\pi(b+I).$$

□

Пример 7.

(a) Пусть $R = \mathcal{F}(M,\mathbb{R})$. Зафиксируем произвольную точку $m_0 \in M$ и рассмотрим гомоморфизм $\varphi\colon R \to \mathbb{R}$, $f \mapsto f(m_0)$. Ясно, что гомоморфизм φ сюръективен. Его ядром является идеал I всех функций, обращающихся в нуль в точке m_0. По теореме о гомоморфизме получаем $R/I \cong \mathbb{R}$.

(b) Рассмотрим отображение $\varphi\colon \mathbb{R}[x] \to \mathbb{C}$, $f \mapsto f(i)$. Очевидно, что φ — гомоморфизм, причем сюръективный. Если функция принадлежит ядру φ, то есть $f(i) = 0$, то $(x-i) \mid f$ в кольце $\mathbb{C}[x]$. Но и сопряженный к корню также будет являться корнем многочлена, так что дополнительно $(x+i) \mid f$. Итого, получаем, что $f \in (x-i)(x+i) = (x^2+1)$ и, соответственно, $\operatorname{Ker}\varphi \subseteq (x^2+1)$. В обратную сторону включение тем более очевидно. Далее, по теореме о гомоморфизме получаем $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Далее в этой лекции всюду предполагается, что R — коммутативное кольцо без делителей нуля.

Определение 43. Говорят, что элемент $b \in R$ *делит* элемент $a \in R$ (b — *делитель* a, a *делится* на b; пишут $b \,|\, a$) если существует элемент $c \in R$, для которого $a = bc$.

Определение 44. Два элемента $a, b \in R$ называются *ассоциированными*, если $a = bc$ для некоторого обратимого элемента c кольца R.

Замечание 23. Легко видеть, что отношение ассоциированности является отношением эквивалентности на кольце R.

Определение 45. Кольцо R без делителей нуля, не являющееся полем, называется ***евклидовым***, если существует функция

$$N \colon R \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$$

(называемая ***нормой***), удовлетворяющая следующим условиям:

1) $N(ab) \geqslant N(a)$ для всех $a, b \in R \setminus \{0\}$;

2) для любых $a, b \in R$, $b \neq 0$, существуют такие $q, r \in R$, что $a = qb + r$ и либо $r = 0$, либо $N(r) < N(b)$.

Неформально говоря, условие 2) означает возможность «деления с остатком» в кольце R.

Примеры евклидовых колец:

1) $\mathbb{Z}$ с нормой $N(a) = |a|$;

2) $K[x]$ (где K — произвольное поле) с нормой $N(f) = \deg f$.

Лемма 7. *Пусть R — евклидово кольцо и $a, b \in R \setminus \{0\}$. Равенство $N(ab) = N(a)$ выполнено тогда и только тогда, когда b обратим.*

Доказательство. Если b обратим, то $N(a) \leqslant N(ab) \leqslant N(abb^{-1}) = N(a)$, откуда $N(ab) = N(a)$.

Пусть теперь $N(ab) = N(a)$. Разделим a на ab с остатком: $a = qab + r$, где либо $r = 0$, либо $N(r) < N(ab)$. Если $r \neq 0$, то с учётом равенства $r = a(1 - qb)$ имеем $N(a) \leqslant N(a(1 - qb)) = N(r) < N(ab) = N(a)$ — противоречие. Значит, $r = 0$ и $a = qab$, откуда $a(1 - qb) = 0$. Так как в R нет делителей нуля и $a \neq 0$, то $1 - qb = 0$, откуда $qb = 1$, т. е. b обратим. □

Определение 46. Кольцо R называется ***кольцом главных идеалов***, если всякий идеал в R является главным.

Теорема 5. *Всякое евклидово кольцо R является кольцом главных идеалов.*

Доказательство. Пусть I — произвольный идеал в R. Если $I = \{0\}$, то $I = (0)$ и поэтому I является главным. Далее считаем, что $I \neq \{0\}$. Пусть $a \in I \setminus \{0\}$ — элемент с наименьшей нормой. Тогда главный идеал (a) содержится в I. Предположим, что какой-то элемент $b \in I$ не лежит в (a), т. е. не делится на a. Тогда разделим b на a с остатком: $b = qa + r$, где $r \neq 0$ и $N(r) < N(a)$. Так как $r = b - aq$, то $r \in I$, что в силу неравенства $N(r) < N(a)$ противоречит нашему выбору элемента a. □

Определение 47. ***Наибольшим общим делителем*** элементов a и b кольца R называется их общий делитель, который делится на любой другой их общий делитель. Он обозначается (a, b).

Замечание 24. Если наибольший общий делитель двух элементов $a, b \in R$ существует, то он определён однозначно с точностью до ассоциированности, т. е. умножения на обратимый элемент кольца R.

Теорема 6. *Пусть R — евклидово кольцо и a, b — произвольные элементы. Тогда:*

(1) *существует наибольший общий делитель (a, b);*

(2) *существуют такие элементы $u, v \in R$, что $(a, b) = ua + vb$.*

Доказательство.
Способ 1: утверждение (1) получается применением (прямого хода) алгоритма Евклида, а утверждение (2) — применением обратного хода в алгоритме Евклида.

Способ 2: рассмотрим идеал $I = (a, b)$. Так как R — кольцо главных идеалов, то существует такой элемент $d \in R$, что $I = (d)$ и существуют $x, y \in R$ такие, что

$$d = ax + dy. \qquad (*)$$

Покажем, что $d = (a, b)$. Для начала, так как a и b лежат в идеале $I = (d)$, то они оба делятся на d, то есть d является одним из их делителей. А из равенства $(*)$ ясно, что любой другой общий делитель a и b будет также делиться на d. Итого, d — наибольший общий делитель. □

Определение 48. Ненулевой необратимый элемент p кольца R называется ***простым***, если он не может быть представлен в виде $p = ab$, где $a, b \in R$ — необратимые элементы.

Замечание 25. Простые элементы в кольце многочленов $K[x]$ над полем K принято называть *неприводимыми многочленами.*

Лемма 8. *Если простой элемент p евклидова кольца R делит произведение $a_1 a_2 \ldots a_n$, то он делит один из сомножителей.*

Доказательство. Индукция по n. Пусть $n = 2$ и предположим, что p не делит a_1. Тогда $(p, a_1) = 1$ и по утверждению (2) теоремы 6 найдутся такие элементы $u, v \in R$, что $1 = up + va_1$. Умножая обе части этого равенства на a_2, получаем

$$a_2 = upa_2 + va_1a_2.$$

Легко видеть, что p делит правую часть последнего равенства, поэтому p делит и левую часть, т. е. a_2.

При $n > 2$ применяем предыдущее рассуждение к $(a_1 \dots a_{n-1})a_n$ и пользуемся предположением индукции. □

Определение 49. Кольцо R называется *факториальным*, если всякий его ненулевой необратимый элемент «разложим на простые множители», т. е. представим в виде произведения (конечного числа) простых элементов, причём это представление единственно с точностью до перестановки множителей и ассоциированности.

Более формально единственность разложения на простые множители следует понимать так: если для элемента $a \in R$ есть два представления

$$a = p_1p_2 \dots p_n = q_1q_2 \dots q_m,$$

где все элементы p_i, q_j простые, то $n = m$ и существует такая подстановка $\sigma \in S_n$, что для каждого $i = 1, \dots, n$ элементы p_i и $q_{\sigma(i)}$ ассоциированы.

Теорема 7. *Всякое евклидово кольцо R является факториальным.*

Доказательство состоит из двух шагов.

Шаг 1. Сначала докажем, что всякий ненулевой необратимый элемент из R разложим на простые множители. Предположим, что это не так, и среди всех элементов, не разложимых на простые множители, выберем элемент a с наименьшей нормой. Тогда a не может быть простым (иначе он разложим в произведение, состоящее из одного простого множителя), поэтому существует представление вида $a = bc$, где $b, c \in R$ — ненулевые необратимые элементы. Но тогда в силу леммы 7 имеем $N(b) < N(a)$ и $N(c) < N(a)$, поэтому элементы b и c разложимы на простые множители. Но тогда и a разложим — противоречие.

Шаг 2. Докажем теперь индукцией по n, что если для некоторого элемента $a \in R$ имеются два разложения

$$a = p_1p_2 \dots p_n = q_1q_2 \dots q_m,$$

где все элемнты p_i и q_j простые, то $m = n$ и после подходящей перенумерации элементов q_j окажется, что при всех $i = 1, \dots, n$ элемент p_i ассоциирован с q_i.

Если $n = 1$, то $a = p_1$; тогда из определения простого элемента следует, что $m = 1$ и тем самым $q_1 = p_1$. Пусть теперь $n > 1$. Тогда элемент p_1 делит произведение $q_1q_2 \dots q_m$. По лемме 8 этот элемент делит некоторый q_i, а значит, ассоциирован с ним. Выполнив перенумерацию, можно считать, что $i = 1$ и $q_1 = cp_1$ для некоторого обратимого элемента $c \in R$. Так как в R нет делителей нуля, то мы можем сократить на p_1, после чего получится равенство

$$p_2p_3 \dots p_n = (cq_2)q_3 \dots q_m$$

(заметьте, что элемент cq_2 прост!). Дальше используем предположение индукции. □

Можно показать (см. листок с задачами к лекции 6), что при $n \geqslant 2$ кольцо многочленов $K[x_1, \dots, x_n]$ над произвольным полем K не является кольцом главных идеалов, а значит, по теореме 5 это кольцо не является евклидовым. Тем не менее, наша цель в оставшейся части этой лекции — доказать, что кольцо $K[x_1, \dots, x_n]$ факториально.

Начнём издалека. С каждым (коммутативным) кольцом R (без делителей нуля) связано его *поле отношений* K. Элементами этого поля являются дроби вида $\frac{a}{b}$, где $a, b \in R$ и $b \neq 0$, со стандартными правилами отождествления ($\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$), сложения ($\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$) и умножения ($\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$). Кольцо R реализуется как подкольцо в K, состоящее из всех дробей вида $\frac{a}{1}$.

Модельный пример: $\mathbb{Q}$ есть поле отношений кольца $\mathbb{Z}$.

Всякий гомоморфизм колец $\varphi\colon R \to R'$ индуцирует гомоморфизм $\widetilde{\varphi}\colon R[x] \to R'[x]$ соответствующих колец многочленов, задаваемый по правилу

$$a_nx^n + a_{n-1}x^{n-1} + \dots a_1x + a_0 \mapsto \varphi(a_n)x^n + \varphi(a_{n-1})x^{n-1} + \dots \varphi(a_1)x + \varphi(a_0).$$

Вспомнив, как определяется умножение в кольце многочленов, легко показать, что $\widetilde{\varphi}$ действительно является гомоморфизмом.

В частности, если R — кольцо и K — его поле частных, то вложение $R \hookrightarrow K$ индуцирует вложение $R[x] \hookrightarrow K[x]$, так что всякий многочлен с коэффициентами из R можно рассматривать как многочлен с коэффициентами из K.

Пусть R — кольцо.

Определение 50. Многочлен $f(x) \in R[x]$ называется *примитивным*, если в R нет необратимого элемента, который делит все коэффициенты многочлена $f(x)$.

Лемма Гаусса. Если R — факториальное кольцо с полем отношений K и многочлен $f(x) \in R[x]$ разлагается в произведение двух многочленов в кольце $K[x]$, то он разлагается в произведение двух пропорциональных им многочленов в кольце $R[x]$.

В доказательстве леммы Гаусса нам потребуются следующие факты.

Упражнение 6. Пусть R — факториальное кольцо и $p \in R$ — простой элемент. Тогда в факторкольце $R/(p)$ нет делителей нуля.

Упражнение 7. Пусть R — (коммутативное) кольцо (без делителей нуля). Тогда в кольце многочленов $R[x]$ также нет делителей нуля.

Доказательство леммы Гаусса. Пусть $f(x) = g(x)h(x)$, где $g(x), h(x) \in K[x]$. Так как кольцо R факториально, то для любого набора элементов из R определены наибольший общий делитель и наименьшее общее кратное. С учётом этого приведём все коэффициенты многочлена $g(x)$ к общему знаменателю, после чего вынесем за скобку этот общий знаменатель и наибольший общий делитель всех числителей. В результате в скобках останется примитивный многочлен $g_1(x) \in R[x]$, а за скобками — некоторый элемент из поля K. Аналогичным образом найдём примитивный многочлен $h_1(x) \in R[x]$, который пропорционален многочлену $h(x)$. Теперь мы можем записать $f(x) = \frac{u}{v} g_1(x)h_1(x)$, где $u, v \in R$, $v \neq 0$ и без ограничения общности можно считать $(u, v) = 1$. Для завершения доказательства достаточно показать, что элемент v обратим (и тогда разложение $f(x) = (uv^{-1}g_1(x))h_1(x)$ будет искомым).

Предположим, что v необратим. Тогда найдётся простой элемент $p \in R$, который делит v. Рассмотрим гомоморфизм факторизации $\varphi\colon R \to R/(p)$, $a \mapsto a + (p)$, и соответствующий ему гомоморфизм колец многочленов $\widetilde{\varphi}\colon R[x] \to (R/(p))[x]$. В кольце $R[x]$ у нас имеется равенство $vf(x) = ug_1(x)h_1(x)$. Взяв образ обеих частей этого равенства при гомоморфизме $\widetilde{\varphi}$, мы получим следующее равенство в кольце $(R/(p))[x]$:

$$\widetilde{\varphi}(v)\widetilde{\varphi}(f(x)) = \widetilde{\varphi}(u)\widetilde{\varphi}(g_1(x))\widetilde{\varphi}(h_1(x)). \tag{11}$$

Поскольку p делит v, имеем $\widetilde{\varphi}(v) = 0$, поэтому левая часть равенства (11) равна нулю. С другой стороны, из условия $(u, v) = 1$ следует, что $\widetilde{\varphi}(u) \neq 0$, а из примитивности многочленов $g_1(x)$ и $h_1(x)$ вытекает, что $\widetilde{\varphi}(g_1(x)) \neq 0$ и $\widetilde{\varphi}(h_1(x)) \neq 0$. Таким образом, все три множителя в правой части равенства (11) отличны от нуля. Из упражнений 6 и 7 вытекает, что в кольце $(R/(p))[x]$ нет делителей нуля, поэтому правая часть равенства (11) отлична от нуля, и мы пришли к противоречию. □

Следствие 11. *Если многочлен $f(x) \in R[x]$ может быть разложен в произведение двух многочленов меньшей степени в кольце $K[x]$, то он может быть разложен и в произведение двух многочленов меньшей степени в кольце $R[x]$.*

Теорема 8. *Если кольцо R факториально, то кольцо многочленов $R[x]$ также факториально.*

Доказательство. Следствие 11 показывает, что простые элементы кольца $R[x]$ — это в точности элементы одного из следующих двух типов:

1) простые элементы кольца R (рассматриваемые как многочлены степени 0 в $R[x]$);

2) примитивные многочлены из $R[x]$, неприводимые над полем отношений K.

Ясно, что каждый многочлен из $R[x]$ разлагается в произведение таких многочленов. Предположим, что какой-то элемент из $R[x]$ двумя способами представим в виде такого произведения:

$$a_1 \ldots a_n b_1(x) \ldots b_m(x) = a'_1 \ldots a'_k b'_1(x) \ldots b'_l(x),$$

где a_i, a'_j — простые элементы типа 1 и $b_i(x), b'_j(x)$ — простые элементы типа 2.

Рассмотрим эти разложения в кольце $K[x]$. Как мы уже знаем из теоремы 7, кольцо $K[x]$ факториально. Отсюда следует, что $m = l$ и после подходящей перенумерации элементов $b'_j(x)$ получается, что при всех $j = 1, \ldots, m$ элементы $b_j(x)$ и $b'_j(x)$ ассоциированы в $K[x]$, а в силу примитивности они ассоциированы и в $R[x]$. После сокращения всех таких элементов у нас останутся два разложения на простые множители (какого-то) элемента из R. Но кольцо R факториально, поэтому эти два разложения совпадают с точностью до перестановки множителей и ассоциированности. □

Теорема 9. *Пусть K — произвольное поле. Тогда кольцо многочленов $K[x_1, \ldots, x_n]$ факториально.*

Доказательство. Воспользуемся индукцией по n. При $n = 1$ наше кольцо евклидово и по теореме 7 факториально. При $n > 1$ имеем $K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$, кольцо $K[x_1, \ldots, x_{n-1}]$ факториально по предположению индукции и требуемый результат следует из предыдущей теоремы. □

Замечание 26. Несмотря на естественность условия единственности разложения на простые множители, большинство колец не являются факториальными. Например, таковым не является кольцо $\mathbb{Z}[\sqrt{-5}]$, состоящее из всех комплексных чисел вида $a + b\sqrt{-5}$, где $a, b \in \mathbb{Z}$: в этом кольце число 6 разлагается на простые множители двумя различными способами: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Лекция 8

Элементарные симметрические многочлены. Основная теорема о симметрических многочленах. Лексикографический порядок. Теорема Виета. Дискриминант многочлена.

Вернемся ненадолго к теме прошлой лекции. Рассмотрим кольцо $R = K[x_1, \dots, x_n]$, где K — поле. На семинарах разбиралось, что оно не является кольцом главных идеалов и, соответственно, евклидовым кольцом. Однако несмотря на это:

Теорема. Кольцо R факториально.

Впрочем, доказывать эту теорему мы не будем.

Вернемся теперь к теме текущей лекции. Пусть K — произвольное поле.

Определение 51. Многочлен $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ называется *симметрическим*, если $f(x_{\tau(1)}, \dots, x_{\tau(n)}) = f(x_1, \dots, x_n)$ для всякой перестановки $\tau \in S_n$.

Примеры:

1) Многочлен $x_1x_2 + x_2x_3$ не является симметрическим, а вот многочлен $x_1x_2 + x_2x_3 + x_1x_3$ — является.

2) *Степенные суммы* $s_k(x_1, \dots, x_n) = x_1^k + x_2^k + \dots + x_n^k$ являются симметрическими многочленами.

3) *Элементарные симметрические многочлены*

$$\sigma_1(x_1, \dots, x_n) = x_1 + x_2 + \dots + x_n;$$

$$\sigma_2(x_1, \dots, x_n) = \sum_{1 \leqslant i < j \leqslant n} x_i x_j;$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \leqslant i_1 < i_2 < \dots < i_k \leqslant n} x_{i_1} x_{i_2} \dots x_{i_k};$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\sigma_n(x_1, \dots, x_n) = x_1 x_2 \dots x_n$$

являются симметрическими.

5) Определитель Вандермонда

$$V(x_1, \dots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)$$

симметрическим многочленом не является (при перестановке индексов умножается на её знак), а вот его квадрат уже является.

Основная цель этой лекции — понять, как устроены все симметрические многочлены.

Легко видеть, что все симметрические многочлены образуют подкольцо (и даже подалгебру) в $K[x_1, \dots, x_n]$. В частности, если $F(y_1, \dots, y_k)$ — произвольный многочлен и $f_1(x_1, \dots, x_n)$, …, $f_k(x_1, \dots, x_n)$ — симметрические многочлены, то многочлен

$$F(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n)) \in K[x_1, \dots, x_n]$$

также является симметрическим. Мы покажем, что всякий симметрический многочлен однозначно выражается через элементарные симметрические многочлены.

Основная теорема о симметрических многочленах. Для всякого симметрического многочлена $f(x_1, \dots, x_n)$ существует и единственен такой многочлен $F(y_1, \dots, y_n)$, что

$$f(x_1, \dots, x_n) = F(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)).$$

Пример. $s_2(x_1, \dots, x_n) = x_1^2 + \dots + x_n^2 = (x_1 + \dots + x_n)^2 - 2 \sum\limits_{1 \leqslant i < j \leqslant n} x_i x_j = \sigma_1^2 - 2\sigma_2$, откуда $F(y_1, \dots, y_n) = y_1^2 - 2y_2$.

Доказательство этой теоремы потребует некоторой подготовки. Начнём с того, что определим старший член многочлена от многих переменных.

Пусть M_n — множество всех одночленов от переменных $x_1, \dots, x_n$. Определим на M_n *лексикографический порядок* следующим образом:

$$a x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \prec b x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} \quad \Leftrightarrow \quad \exists k : \ i_1 = j_1, \dots, i_{k-1} = j_{k-1}, i_k < j_k.$$

Например, $x_1^2 x_3^9 \prec x_1^2 x_2$.

Свойства:

1) Лексикографический порядок обладает свойством транзитивности: если $u, v, w \in M_n$, $u \prec v$ и $v \prec w$, то $u \prec w$ (докажите это).

2) Если $u, v, w \in M_n$ и $u \prec v$, то $uw \prec vw$.

Свойство транзитивности лексикографического порядка позволяет корректно определить следующее понятие.

Определение 52. *Старшим членом* ненулевого многочлена $f(x_1, \ldots, x_n)$ называется наибольший в лексикографическом порядке встречающий в нём одночлен. Обозначение: $L(f)$.

Примеры:

1) $L(s_k) = x_1^k$;

2) $L(\sigma_k) = x_1 x_2 \ldots x_k$.

Лемма о старшем члене. Пусть $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ — произвольные ненулевые многочлены. Тогда $L(fg) = L(f)L(g)$.

Доказательство. Пусть u — какой-то одночлен многочлена f и v — какой-то одночлен многочлена g. По определению старшего члена имеем

$$u \preccurlyeq L(f), \quad v \preccurlyeq L(g). \tag{12}$$

Тогда $uv \preccurlyeq uL(g) \preccurlyeq L(f)L(g)$, т. е. $uv \preccurlyeq L(f)L(g)$. Более того, легко видеть, что $uv \prec L(f)L(g)$ тогда и только тогда, когда хотя бы одно из «неравенств» (12) является строгим. Отсюда следует, что после раскрытия скобок в произведении fg одночлен $L(f)L(g)$ будет старше всех остальных возникающих одночленов. Ясно, что после приведения подобных членов этот одночлен сохранится и будет по-прежнему старше всех остальных одночленов, поэтому $L(f)L(g) = L(fg)$. □

Лемма 9. *Если $ax_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ — старший член некоторого симметрического многочлена $f(x_1, \ldots, x_n)$, то $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$.*

Доказательство. От противного. Пусть $k_i < k_{i+1}$ для некоторого $i \in \{1, \ldots, n-1\}$. Тогда, будучи симметрическим, многочлен f содержит одночлен $ax_1^{k_1} \ldots x_{i-1}^{k_{i-1}} x_i^{k_{i+1}} x_{i+1}^{k_i} x_{i+2}^{k_{i+2}} \ldots x_n^{k_n}$, который старше $L(f)$. Противоречие. □

Лемма 10. *Пусть $k_1, \ldots, k_n$ — целые неотрицательные числа. Если $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$, то существуют и единственны такие целые неотрицательные числа $l_1, l_2, \ldots, l_n$, что*

$$x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = L(\sigma_1(x_1, \ldots, x_n)^{l_1} \sigma_2(x_1, \ldots, x_n)^{l_2} \ldots \sigma_n(x_1, \ldots, x_n)^{l_n}).$$

Доказательство. С учётом леммы о старшем члене требуемое условие означает, что искомые числа $l_1, \ldots, l_n$ удовлетворяют системе

$$\begin{cases} l_1 + l_2 + \ldots + l_n = k_1; \\ \qquad l_2 + \ldots + l_n = k_2; \\ \qquad\qquad \ldots\ldots\ldots\ldots \\ \qquad\qquad\qquad l_n = k_n, \end{cases}$$

из которой они легко находятся:

$$\begin{aligned} &l_i = k_i - k_{i+1} \quad \text{при } 1 \leqslant i \leqslant n-1; \\ &l_n = k_n. \end{aligned}$$

□

Доказательство основной теоремы о симметрических многочленах. Пусть $f(x_1, \ldots, x_n)$ — произвольный симметрический многочлен.

Сначала докажем существование искомого многочлена $F(y_1, \ldots, y_n)$. Если $f(x_1, \ldots, x_n)$ — нулевой многочлен, то можно взять $F(y_1, \ldots, y_n) = 0$. Далее считаем, что $f(x_1, \ldots, x_n) \neq 0$. Пусть $L(f) = ax_1^{k_1} \ldots x_n^{k_n}$, $a \neq 0$. Тогда $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$ в силу леммы 9. По лемме 10 найдётся одночлен от элементарных симметрических многочленов $a\sigma_1^{l_1} \ldots \sigma_n^{l_n}$, старший член которого совпадает с $L(f)$. Положим $f_1 := f - a\sigma_1^{l_1} \ldots \sigma_n^{l_n}$. Если $f_1 = 0$, то $f = a\sigma_1^{l_1} \ldots \sigma_n^{l_n}$ и искомым многочленом будет $F(y_1, \ldots, y_n) = ay_1^{l_1} \ldots y_n^{l_n}$. Если же $f_1 \neq 0$, то $L(f_1) \prec L(f)$. Повторим ту же процедуру: вычтя из f_1 подходящий одночлен от $\sigma_1, \ldots, \sigma_n$, мы получим новый многочлен f_2 со следующим свойством: либо $f_2 = 0$ (и тогда мы получаем выражение f через элементерные симметрические многочлены), либо $L(f_2) \prec L(f_1)$. Многократно повторяя эту процедуру, мы получим последовательность многочленов $f, f_1, f_2, \dots$ со свойством $L(f) \succ L(f_1) \succ L(f_2) \succ \dots$. Покажем, что процесс закончится, т. е. найдётся такое m, что $f_m = 0$ (и тогда мы получим представление f в виде многочлена от $\sigma_1, \dots, \sigma_n$). Для этого заметим, что переменная x_1 входит в старший член каждого из многочленов $f_1, f_2, \dots$ в степени, не превышающей k_1. Но в силу леммы 9 одночленов с таким условием имеется лишь конечное число, поэтому процесс не может продолжаться бесконечно.

Теперь докажем единственность многочлена $F(y_1, \dots, y_n)$. Предположим, что

$$f(x_1, \dots, x_n) = F(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n) = G(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n))$$

для двух различных многочленов $F(y_1, \dots, y_n), G(y_1, \dots, y_n) \in K[y_1, \dots, y_n]$. Тогда многочлен

$$H(y_1, \dots, y_n) := F(y_1, \dots, y_n) - G(y_1, \dots, y_n)$$

является ненулевым, но $H(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) = 0$. Покажем, что такое невозможно. Пусть $H_1, \dots, H_s$ — все ненулевые одночлены в H. Обозначим через w_i старший член многочлена

$$H_i(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) \in K[x_1, \dots, x_n].$$

В силу леммы 10 среди одночленов $w_1, \dots, w_s$ нет пропорциональных. Выберем из них старший в лексикографическом порядке. Он не может сократиться ни с одним членов в выражении

$$H_1(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) + \ldots + H_s(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)),$$

поэтому $H(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) \neq 0$, и мы пришли к противоречию. $\square$

На практике многочлен $F(y_1, \dots, y_n)$ можно искать, повторяя описанный в доказательстве алгоритм, однако он может потребовать много вычислений. Более эффективным для нахождения многочлена $F(y_1, \dots, y_n)$ является метод неопределённых коэффициентов, который планируется разобрать на семинарах.

Теорема Виета. Пусть $\alpha_1, \dots, \alpha_n$ — корни многочлена $x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$. Тогда

$$\sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k a_{n-k}, \quad k = 1, \dots, n.$$

Доказательство. Достаточно приравнять коэффициенты при x^{n-k} в левой и правой частях равенства

$$x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

$\square$

Из теоремы Виета и основной теоремы о симметрических многочленах следует, что мы можем выразить значение любого симметрического многочлена от корней данного многочлена через коэффициенты, не находя самих корней.

Определение 53. *Дискриминантом* многочлена $h(x) = a_n x^n + \ldots + a_1 x + a_0$ с корнями $\alpha_1, \dots, \alpha_n$ называется выражение

$$D(h) = a_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

Замечание 27. Дискриминант $D(h)$ является симметрическим многочленом от $\alpha_1, \dots, \alpha_n$, а значит, в соответствии с вышесказанным он является многочленом от коэффициентов $a_n, a_{n-1}, \dots, a_0$.

Замечание 28. Непосредствено из определения следует, что $D(h) = 0$ тогда и только тогда, когда многочлен h имеет кратный корень.

Лекция 9

Примеры полей. Характеристика поля. Расширения полей, алгебраические и трансцендентные элементы. Минимальные многочлен. Конечное расширение и его степень. Присоединение корня многочлена. Поле разложения многочлена: существование и единственность.

Мы знаем не так много примеров полей. Это бесконечные поля $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ и конечные поля $\mathbb{Z}_p$, где p — простое число. Конструкция поля отношений позволяет строить новые поля из уже имеющихся. А именно, если K — произвольное поле, то можно рассмотреть поле отношений $K(x)$ кольца многочленов $K[x]$ (это поле называется *полем рациональных дробей* над K). Элементами поля $K(x)$ являются дроби $f(x)/g(x)$, где $f(x), g(x) \in K[x]$ и $g(x) \neq 0$.

Несколько других примеров полей:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}, \quad \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}, \quad \mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}.$$

Определение 54. Пусть K — произвольное поле. *Характеристикой* поля K называется такое наименьшее натуральное число p, что $\underbrace{1 + \ldots + 1}_{p} = 0$. Если такого натурального p не существует, говорят, что характеристика поля равна нулю. Обозначение: $\operatorname{char} K$.

Например, $\operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = 0$ и $\operatorname{char}\mathbb{Z}_p = \operatorname{char}\mathbb{Z}_p(x) = p$.

Из определения следует, что всякое поле характеристики нуль бесконечно. Примером бесконечного поля характеристики $p > 0$ является поле $\mathbb{Z}_p(x)$.

Предложение 11. *Характеристика произвольного поля K либо равна нулю, либо является простым числом.*

Доказательство. Положим $p = \operatorname{char} K$ и предположим, что $p > 0$. Так как $0 \neq 1$ в K, то $p \geqslant 2$. Если число p не является простым, то $p = mk$ для некоторых $m, k \in \mathbb{N}$, $1 < m, k < p$. Тогда в K верно равенство

$$0 = \underbrace{1 + \ldots + 1}_{mk} = (\underbrace{1 + \ldots + 1}_{m})(\underbrace{1 + \ldots + 1}_{k}).$$

В силу минимальности числа p в последнем выражении обе скобки отличны от нуля, но такое невозможно, так как в поле нет делителей нуля. $\square$

Упражнение 8. Пересечение любого семейства подполей фиксированного поля K является подполем в K. В частности, для всякого подмножества $S \subseteq K$ существует наименьшее по включению подполе в K, содержащее S. Это подполе совпадает с пересечением всех подполей в K, содержащих S.

Из приведённого выше упражнения следует, что в каждом поле существует наименьшее по включению подполе, оно называется *простым подполем.*

Предложение 12. *Пусть K — поле и K_0 — его простое подполе. Тогда:*

(1) *если* $\operatorname{char} K = p > 0$, *то* $K_0 \cong \mathbb{Z}_p$;

(2) *если* $\operatorname{char} K = 0$, *то* $K_0 \cong \mathbb{Q}$.

Доказательство. Пусть $\langle 1 \rangle \subseteq K$ — циклическая подгруппа по сложению, порождённая единицей. Заметим, что $\langle 1 \rangle$ — подкольцо в K. Поскольку всякое подполе поля K содержит единицу, оно содержит и множество $\langle 1 \rangle$. Следовательно, $\langle 1 \rangle \subseteq K_0$.

Если $\operatorname{char} K = p > 0$, то мы имеем изоморфизм колец $\langle 1 \rangle \simeq \mathbb{Z}_p$. Но, как мы уже знаем из лекции 6, кольцо $\mathbb{Z}_p$ является полем, поэтому $K_0 = \langle 1 \rangle \simeq \mathbb{Z}_p$.

Если же $\operatorname{char} K = 0$, то мы имеем изоморфизм колец $\langle 1 \rangle \cong \mathbb{Z}$. Тогда K_0 содержит все дроби вида a/b, где $a, b \in \langle 1 \rangle$ и $b \neq 0$. Ясно, что все такие дроби образуют поле, изоморфное полю $\mathbb{Q}$. $\square$

Определение 55. Если K — подполе поля F, то говорят, что F — *расширение* поля K.

Например, всякое поле есть расширение своего простого подполя.

Определение 56. *Степенью* расширения полей $K \subseteq F$ называется размерность поля F как векторного пространства над полем K. Обозначение $[F : K]$.

Например, $[\mathbb{C} : \mathbb{R}] = 2$ и $[\mathbb{R} : \mathbb{Q}] = \infty$.

Определение 57. Расширение полей $K \subseteq F$ называется *конечным*, если $[F : K] < \infty$.

Предложение 13. *Пусть $K \subseteq F$ и $F \subseteq L$ — конечные расширения полей. Тогда расширение $F \subseteq L$ также конечно и $[L : K] = [L : F][F : K]$.*

Доказательство. Пусть $e_1, \ldots, e_n$ — базис F над K и $f_1, \ldots, f_m$ — базис L над F. Достаточно доказать, что множество

$$\{e_i f_j \mid i = 1, \ldots, n;\ j = 1, \ldots, m\} \tag{13}$$

является базисом L над K. Для этого сначала покажем, что произвольный элемент $a \in L$ представим в виде линейной комбинации элементов (13) с коэффициентами из K. Поскольку $f_1, \ldots, f_m$ — базис L над F, имеем $a = \sum\limits_{j=1}^{m} \alpha_j f_j$ для некоторых $\alpha_j \in F$. Далее, поскольку $e_1, \ldots, e_n$ — базис F над K, для каждого $j = 1, \ldots, m$ имеем $\alpha_j = \sum\limits_{i=1}^{n} \beta_{ij} e_i$ для некоторых $\beta_{ij} \in K$. Отсюда получаем, что $a = \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} \beta_{ij}(e_i f_j)$.

Теперь проверим линейную независимость элементов (13). Пусть $\sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} \gamma_{ij}(e_j f_i) = 0$, где $\gamma_{ij} \in K$. Переписав это равенство в виде $\sum\limits_{j=1}^{m} (\sum\limits_{i=1}^{n} \gamma_{ij} e_i) f_j = 0$ и воспользовавшись тем, что элементы $f_1, \ldots, f_m$ линейно независимы над F, мы получим $\sum\limits_{i=1}^{n} \gamma_{ij} e_i = 0$ для каждого $j = 1, \ldots, m$. Теперь из линейной независимости элементов $e_1, \ldots, e_n$ над K вытекает, что $\gamma_{ij} = 0$ при всех i, j. Таким образом, элементы (13) линейно независимы. □

Пусть $K \subseteq F$ — расширение полей.

Определение 58. Элемент $\alpha \in F$ называется *алгебраическим* над подполем K, если существует ненулевой многочлен $f(x) \in K[x]$, для которого $f(\alpha) = 0$. В противном случае α называется *трансцендентным* элементом над K.

Определение 59. *Минимальным многочленом* алгебраического элемента $\alpha \in F$ над подполем K называется ненулевой многочлен $h_\alpha(x)$ наименьшей степени, для которого $h_\alpha(\alpha) = 0$.

Лемма 11. *Пусть $\alpha \in F$ — алгебраический элемент над K и $h_\alpha(x)$ — его минимальный многочлен. Тогда:*

(а) *$h_\alpha(x)$ определён однозначно с точностью до пропорциональности;*

(б) *$h_\alpha(x)$ является неприводимым многочленом над полем K;*

(в) *для произвольного многочлена $f(x) \in K[x]$ равенство $f(\alpha) = 0$ имеет место тогда и только тогда, когда $h_\alpha(x)$ делит $f(x)$.*

Доказательство. (а) Пусть $h'_\alpha(x)$ — ещё один минимальный многочлен элемента α над K. Тогда $\deg h_\alpha(x) = \deg h'_\alpha(x)$. Умножив многочлены $h_\alpha(x)$ и $h'_\alpha(x)$ на подходящие константы, добьёмся того, чтобы их старшие коэффициенты стали равны единице. После этого положим $g(x) = h_\alpha(x) - h'_\alpha(x)$. Тогда $g(\alpha) = 0$ и $\deg g(x) < \deg h_\alpha(x)$. Учитывая определение минимального многочлена, мы получаем $g(x) = 0$.

(б) Пусть $h_\alpha(x) = h_1(x)h_2(x)$ для некоторых $h_1(x), h_2(x) \in K[x]$, причём $0 < \deg h_i(x) < \deg h_\alpha(x)$ при $i = 1, 2$. Так как $h_\alpha(\alpha) = 0$, то либо $h_1(\alpha) = 0$, либо $h_2(\alpha) = 0$, что противоречит минимальности $h_\alpha(x)$.

(в) Очевидно, что если $h_\alpha(x)$ делит $f(x)$, то $f(\alpha) = 0$. Докажем обратное утверждение. Разделим $f(x)$ на $h_\alpha(x)$ с остатком: $f(x) = q(x)h_\alpha(x) + r(x)$, где $q(x), r(x) \in K[x]$ и $\deg r(x) < \deg h_\alpha(x)$. Тогда условие $f(\alpha) = 0$ влечёт $r(\alpha) = 0$. Из минимальности многочлена $h_\alpha(x)$ получаем $r(x) = 0$. □

Для каждого элемента $\alpha \in F$ обозначим через $K(\alpha)$ наименьшее подполе в F, содержащее K и α.

Предложение 14. *Пусть $\alpha \in F$ — алгебраический элемент над K и n — степень его минимального многочлена над K. Тогда*

$$K(\alpha) = \{\beta_0 + \beta_1\alpha + \ldots + \beta_{n-1}\alpha^{n-1} \mid \beta_0, \ldots, \beta_{n-1} \in K\}.$$

Кроме того, элементы $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ линейно независимы над K. В частности, $[K(\alpha) : K] = n$.

Доказательство. Легко видеть, что

$$K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \mid f(x), g(x) \in K[x], f(\alpha) \neq 0\}.$$

Действительно, такие элементы лежат в любом подполе поля F, содержащем K и α, и сами образуют поле. Теперь возьмём произвольный элемент $\frac{f(\alpha)}{g(\alpha)} \in K(\alpha)$ и покажем, что он представим в виде, указанном в условии. Пусть $h_\alpha(x) \in K[x]$ — минимальный многочлен элемента α над K. Поскольку $g(\alpha) \neq 0$, в силу леммы 11(в) многочлен $h_\alpha(x)$ не делит $g(x)$. Но $h_\alpha(x)$ неприводим по лемме 11(б), поэтому $(g(x), h_\alpha(x)) = 1$. Значит, существуют такие многочлены $u(x), v(x) \in K[x]$, что $u(x)g(x) + v(x)h_\alpha(x) = 1$. Подставляя в последнее равенство $x = \alpha$, мы получаем $u(\alpha)g(\alpha) = 1$. Отсюда $\frac{f(\alpha)}{g(\alpha)} = f(\alpha)u(\alpha)$, и мы избавились от знаменателя. Теперь уменьшим степень числителя. Пусть $r(x)$ — остаток от деления $f(x)u(x)$ на $h_\alpha(x)$. Тогда $f(\alpha)u(\alpha) = r(\alpha)$ и, значит, $\frac{f(\alpha)}{g(\alpha)} = r(\alpha)$, что показывает представимость элемента $\frac{f\alpha)}{g(\alpha)}$ в требуемом виде.

Остаётся показать, что элементы $1, \alpha, \ldots, \alpha^{n-1}$ поля F линейно независимы над K. Если

$$\gamma_0 + \gamma_1\alpha + \ldots + \gamma_{n-1}\alpha^{n-1} = 0$$

для некоторых $\gamma_0, \gamma_1, \ldots, \gamma_{n-1} \in K$, то для многочлена $w(x) = \gamma_0 + \gamma_1 x + \ldots + \gamma_{n-1}x^{n-1} \in K[x]$ получаем $w(\alpha) = 0$. Тогда из леммы 11(в) и условия $\deg w(x) < \deg h_\alpha(x)$ вытекает, что $w(x) = 0$, то есть $\gamma_0 = \gamma_1 = \ldots = \gamma_{n-1} = 0$. □

Теорема 10. *Пусть K — произвольное поле и $f(x) \in K[x]$ — многочлен положительной степени. Тогда существует конечное расширение $K \subseteq F$, в котором многочлен $f(x)$ имеет корень.*

Доказательство. Достаточно построить конечное расширение, в котором имеет корень один из неприводимых делителей $p(x)$ многочлена $f(x)$.

Покажем сначала, что факторкольцо $K[x]/(p(x))$ является полем. В самом деле, если многочлен $g(x) \in K[x]$ не делится на $p(x)$, то $(g(x), p(x)) = 1$, и тогда существуют многочлены $u(x), v(x) \in K[x]$, для которых $u(x)g(x) + v(x)p(x) = 1$. Взяв образ последнего равенства в факторкольце $K[x]/(p(x))$, мы получим

$$(u(x) + (p(x)))(g(x) + (p(x))) = 1 + (p(x)),$$

т. е. элемент $u(x) + (p(x))$ является обратным к $g(x) + (p(x))$. Значит, $K[x]/(p(x))$ — поле, и мы возьмём его в качестве F.

Заметим теперь, что расширение $K \subseteq F$ является конечным. Действительно, для всякого многочлена $g(x) \in K[x]$ в поле $F = K[x]/(p(x))$ имеем $g(x) + (p(x)) = r(x) + (p(x))$, где $r(x)$ — остаток от деления $g(x)$ на $p(x)$. Отсюда следует, что F порождается как векторное пространство над K элементами

$$1 + (p(x)), x + (p(x)), \ldots, x^{n-1} + (p(x)),$$

где $n = \deg p(x)$. (Так же легко показать, что эти элементы образуют базис в F над K.)

Остаётся показать, что в поле F многочлен $p(x)$ имеет корень. Это похоже на обман, но корнем будет... $x + (p(x))$. Действительно, пусть $p(x) = a_n x^n + a_{n-1}x^{n-1} + a_1 x + a_0$, где $a_0, a_1, \ldots, a_n \in K$. Тогда

$$\begin{aligned} p(x + (p(x))) &= a_n(x + (p(x)))^n + a_{n-1}(x + (p(x)))^{n-1} + \ldots + a_1(x + (p(x)) + a_0 = \\ &= (a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0) + (p(x)) = p(x) + (p(x)) = (p(x)), \end{aligned}$$

а $(p(x))$ есть не что иное, как нуль в F. □

Говорят, что поле $K[x]/(p(x))$ получено из поля K *присоединением корня* неприводимого многочлена $p(x)$. Нетрудно проверить, что если α — некоторый корень многочлена $p(x)$ в $K[x]/(p(x))$, то поле $K[x]/(p(x))$ совпадает с подполем $K(\alpha)$.

Определение 60. Пусть K — некоторое поле и $f(x) \in K[x]$ — многочлен положительной степени. *Полем разложения* многочлена $f(x)$ называется такое расширение F поля K, что

(1) многочлен $f(x)$ разлагается над F на линейные множители;

(2) корни многочлена $f(x)$ не лежат ни в каком собственном подполе поля F, содержащем K.

Пример 8. Рассмотрим многочлен $f(x) = x^4 + x^3 + x^2 + x + 1$ над $\mathbb{Q}$. Так как $(x-1)f(x) = x^5 - 1$, корнями многочлена $f(x)$ являются все корни степени 5 из единицы, отличные от единицы. Если присоединить к $\mathbb{Q}$ один из корней ϵ многочлена f, то его остальные корни можно получить, возводя число ϵ в натуральные степени. Таким образом, присоединение одного корня сразу приводит к полю разложения многочлена.

Пример 9. Многочлен $f(x) = x^3 - 2$ неприводим над полем $\mathbb{Q}$. Присоединение к полю $\mathbb{Q}$ корня этого многочлена приводит к полю $\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2})$. Данное поле не является полем разложения многочлена $f(x)$, поскольку в нём $f(x)$ имеет только один корень и не имеет двух других корней. Поскольку корнями данного многочлена являются числа

$$\sqrt[3]{2}, \quad \sqrt[3]{2}(-\frac{1}{2} + \frac{\sqrt{-3}}{2}), \quad \sqrt[3]{2}(-\frac{1}{2} - \frac{\sqrt{-3}}{2}),$$

полем разложения многочлена $f(x)$ является поле

$$F = \{\alpha_0 + \alpha_1 \sqrt[3]{2} + \alpha_2 \sqrt[3]{4} + \alpha_3 \sqrt{-3} + \alpha_4 \sqrt[3]{2}\sqrt{-3} + \alpha_5 \sqrt[3]{4}\sqrt{-3} \mid \alpha_i \in \mathbb{Q}\},$$

которое имеет над $\mathbb{Q}$ степень 6.

Пусть F и F' — два расширения поля K. Говорят, что изоморфизм $F \xrightarrow{\sim} F'$ является *тождественным на* K, если при этом изоморфизме каждый элемент поля K переходит в себя.

Теорема 11. *Поле разложения любого многочлена $f(x) \in K[x]$ существует и единственно с точностью до изоморфизма, тождественного на K.*

Доказательство этой теоремы можно найти, например, в книге Э. Б. Винберга «Курс алгебры». Мы не включаем это доказательство в программу нашего курса.

Лекция 10

Конечные поля. Простое подполе и порядок конечного поля. Автоморфизм Фробениуса. Теорема существования и единственности для конечных полей. Поле из четырех элементов. Цикличность мультипликативной группы. Неприводимые многочлены над конечным полем. Подполя конечного поля.

В этой лекции будем использовать следующее обозначение: $K^\times = K \setminus \{0\}$ — мультипликативная группа поля K.

Пусть K — конечное поле. Тогда его характеристика отлична от нуля и потому равна некоторому простому числу p. Значит, K содержит поле $\mathbb{Z}_p$ в качестве простого подполя.

Теорема 12. *Число элементов конечного поля равно p^n для некоторого простого p и натурального n.*

Доказательство. Пусть K — конечное поле характеристики p, и пусть размерность K над простым подполем $\mathbb{Z}_p$ равна n. Выберем в K базис $e_1, \ldots, e_n$ над $\mathbb{Z}_p$. Тогда каждый элемент из K однозначно представляется в виде $\alpha_1 e_1 + \ldots + \alpha_n e_n$, где $\alpha_1, \ldots, \alpha_n$ пробегают $\mathbb{Z}_p$. Следовательно, в K ровно p^n элементов. $\square$

Пусть K — произвольное поле характеристики $p > 0$. Рассмотрим отображение

$$\varphi\colon K \to K, \quad a \mapsto a^p.$$

Покажем, что φ — гомоморфизм. Для любых $a, b \in K$ по формуле бинома Ньютона имеем

$$(a+b)^p = a^p + C_p^1 a^{p-1} b + C_p^2 a^{p-2} b^2 + \ldots + C_p^{p-1} a b^{p-1} + b^p.$$

Так как p — простое число, то все биномиальные коэффициенты C_p^i при $1 \leqslant i \leqslant p-1$ делятся на p. Это значит, что в нашем поле характеристики p все эти коэффициенты обнуляются, в результате чего получаем $(a+b)^p = a^p + b^p$. Ясно, что $(ab)^p = a^p b^p$, так что φ — гомоморфизм. Ядро любого гомоморфизма колец является идеалом, поэтому $\operatorname{Ker}\varphi$ — идеал в K. Но в поле нет собственных идеалов, поэтому $\operatorname{Ker}\varphi = \{0\}$, откуда φ инъективен.

Если поле K конечно, то инъективное отображение из K в K автоматически биективно. В этой ситуации φ называется *автоморфизмом Фробениуса* поля K.

Замечание 29. Пусть K — произвольное поле и ψ — произвольный автоморфизм (т. е. изоморфизм на себя) поля K. Легко видеть, что множество неподвижных точек $K^\psi = \{a \in K \mid \psi(a) = a\}$ является подполем в K.

Прежде чем перейти к следующей теореме, обсудим понятие формальной производной многочлена. Пусть $K[x]$ — кольцо многочленов над произвольным полем K. Формальной производной называется отображение $K[x] \to K[x]$, которое каждому многочлену $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ сопоставляет многочлен $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + a_1$. Из определения следует, что это отображение линейно. Легко проверить, что для любых $f, g \in K[x]$ справедливо привычное нам равенство $(fg)' = f'g + fg'$ (в силу дистрибутивности умножения проверка этого равенства сводится к случаю, когда f, g — одночлены). В частности, $(f(x)^m)' = m f(x)^{m-1}$ для любых $f(x) \in K[x]$ и $m \in \mathbb{N}$.

Теорема 13. *Для всякого простого числа p и натурального числа n существует единственное (с точностью до изоморфизма) поле из p^n элементов.*

Доказательство. Положим $q = p^n$ для краткости.

Единственность. Пусть поле K содержит q элементов. Тогда мультипликативная группа $K^\times$ имеет порядок $q-1$. По следствию 3 из теоремы Лагранжа мы имеем $a^{q-1} = 1$ для всех $a \in K \setminus \{0\}$, откуда $a^q - a = 0$ для всех $a \in K$. Это значит, что все элементы поля K являются корнями многочлена $x^q - x \in \mathbb{Z}_p[x]$. Отсюда следует, что K является полем разложения многочлена $x^q - x$ над $\mathbb{Z}_p$. Из теоремы о полях разложения, формулировавшейся на прошлой лекции, следует, что поле K единственно с точностью до изоморфизма.

Существование. Пусть K — поле разложения многочлена $f(x) = x^q - x \in \mathbb{Z}_p[x]$. Тогда имеем $f'(x) = q x^{q-1} - 1 = -1$ ($q x^{q-1}$ обнуляется, так как q делится на p, а p — характеристика поля $\mathbb{Z}_p$). Покажем, что многочлен $f(x)$ не имеет кратных корней в K. Действительно, если α — корень кратности $m \geqslant 2$, то $f(x) = (x-\alpha)^m g(x)$ для некоторого многочлена $g(x) \in \mathbb{Z}_p[x]$. Но тогда $f'(x) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x)$, откуда видно, что $f'(x)$ делится на $(x-\alpha)$. Но последнее невозможно, ибо $f'(x) = -1$ — многочлен нулевой степени. Итак, многочлен $f(x)$ имеет ровно q различных корней в поле K. Заметим, что эти корни — в точности неподвижные точки автоморфизма $\varphi^n = \underbrace{\varphi \circ \ldots \circ \varphi}_{n}$, где φ — автоморфизм Фробениуса.

В самом деле, для элемента $a \in K$ равенство $a^q - a = 0$ выполнено тогда и только тогда, когда $a^{p^n} = a$, т. е. $\varphi^n(a) = a$. Значит, корни многочлена $x^q - x$ образуют подполе в K, которое по определению поля разложения совпадает с K. Следовательно, в поле K ровно q элементов. $\square$

Конечные поля еще называют *полями Галуа*. Поле из q элементов обозначают $\mathbb{F}_q$. Например, $\mathbb{F}_p \cong \mathbb{Z}_p$.

Пример 10. Построим явно поле из четырёх элементов. Многочлен x^2+x+1 неприводим над $\mathbb{Z}_2$. Значит, факторкольцо $\mathbb{Z}_2[x]/(x^2+x+1)$ является полем и его элементы — это классы $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}$ (запись $\overline{a}$ означает класс элемента a в факторкольце $\mathbb{Z}_2[x]/(x^2+x+1)$). Например, произведение $\overline{x} \cdot \overline{x+1}$ — это класс элемента x^2+x, который равен $\overline{1}$.

Предложение 15. *Мультипликативная группа конечного поля $\mathbb{F}_q$ является циклической.*

Доказательство. Заметим, что $\mathbb{F}_q^\times$ — конечная абелева группа, и обозначим через m её экспоненту (см. конец лекции 4). Предположим, что группа $\mathbb{F}_q^\times$ не является циклической. Тогда $m < q-1$ по следствию 2 лекции 4. По определению экспоненты это значит, что $a^m = 1$ для всех $a \in \mathbb{F}_q^\times$. Но тогда многочлен $x^m - 1$ имеет в поле $\mathbb{F}_q$ больше корней, чем его степень, — противоречие. $\square$

Теорема 14. *Конечное поле $\mathbb{F}_q$, где $q = p^n$, можно реализовать в виде $\mathbb{Z}_p[x]/(h(x))$, где $h(x)$ — неприводимый многочлен степени n над $\mathbb{Z}_p$. В частности, для всякого $n \in \mathbb{N}$ в кольце $\mathbb{Z}_p[x]$ есть неприводимый многочлен степени n.*

Доказательство. Пусть α — порождающий элемент группы $\mathbb{F}_q^\times$. Тогда минимальное подполе $\mathbb{Z}_p(\alpha)$ поля $\mathbb{F}_q$, содержащее α, совпадает с $\mathbb{F}_q$. Значит, поле $\mathbb{F}_q$ изоморфно полю $\mathbb{Z}_p[x]/(h(x))$, где $h(x)$ — минимальный многочлен элемента α над $\mathbb{Z}_p$. Из результатов прошлой лекции следует, что многочлен $h(x)$ неприводим. Поскольку степень расширения $[\mathbb{F}_q : \mathbb{Z}_p]$ равна n, этот многочлен имеет степень n. $\square$

Теорема 15. *Всякое подполе поля $\mathbb{F}_q$, где $q = p^n$, изоморфно $\mathbb{F}_{p^m}$, где m — делитель числа n. Обратно, для каждого делителя m числа n в поле $\mathbb{F}_q$ существует ровно одно подполе из p^m элементов.*

Доказательство. Пусть F — подполе поля $\mathbb{F}_q$. По определению простого подполя имеем $F \supset \mathbb{Z}_p$, откуда $\operatorname{char} F = p$. Тогда теорема 12 нам сообщает, что $|F| = p^m$ для некоторого $m \in \mathbb{N}$. По теореме 13 имеем $F \cong \mathbb{F}_{p^m}$. Обозначим через s степень (конечного) расширения $F \subset \mathbb{F}_q$. Рассуждая так же, как в доказательстве теоремы 12, мы получим $p^n = (p^m)^s$, откуда $p^n = p^{ms}$ и m делит n.

Пусть теперь m — делитель числа n, т. е. $n = ms$ для некоторого $s \in \mathbb{N}$. Рассмотрим многочлены $f(x) = x^{p^n} - x$ и $g(x) = x^{p^m} - x$ над $\mathbb{Z}_p$. Заметим, что для элемента $a \in \mathbb{F}_q$ равенства $a^{p^m} = a$ следует

$$a^{p^n} = a^{p^{ms}} = a^{(p^m)^s} = (\ldots((a^{p^m})^{p^m})^{p^m}\ldots)^{p^m} \text{ (s раз возвели в степень p^m)} = a.$$

Поэтому каждый корень многочлена $g(x)$ является и корнем многочлена $f(x)$. Отсюда поле разложения многочлена $f(x)$ лежит в поле разложения многочлена $g(x)$. Значит, $\mathbb{F}_{p^m}$ содержится в $\mathbb{F}_{p^n}$.

Наконец, все элементы подполя из p^m элементов неподвижны при автоморфизме $\psi = \underbrace{\varphi \circ \ldots \circ \varphi}_{m} \colon x \mapsto x^{p^m}$ (φ — автоморфизм Фробениуса). Поскольку число корней многочлена $x^{p^m} - x$ в поле $\mathbb{F}_q$ не превосходит p^m, множество элементов данного подполя совпадает с множеством неподвижных точек автоморфизма ψ. Значит, такое подполе единственно. $\square$