Теория групп. Лекция 15

Штепин Вадим Владимирович

12 декабря 2019 г.

1 Периодическая часть группы

Пусть G — конечнопорожденная абелева группа относительно сложения.

Опр. **Периодическая часть группы G (кручение G)** $Tor(G) = \{a \in G \mid ord(a) < \infty\}$.

Утв.

$Tor(G) \leq G$

Доказательство

Пусть $a_1, a_2 \in Tor(G)$. Тогда $\exists n_1, n_2$ $n_1 a_1 = n_2 a_2 = 0$. Очевидно, что $n_1 n_2 (a_1 + a_2) = 0 \Rightarrow a_1 + a_2 \in Tor(G)$. Более того, $ord(a_1 + a_2) | ord(a_1) ord(a_2)$. Аналогично, $-a_1 \in Tor(G)$.

Утв.

Пусть $G = H \oplus Z^k$, где H — прямая сумма примарных циклических подгрупп $H = Z_{p_1^{\alpha_1}} \oplus ... \oplus Z_{p_s^{\alpha_s}}$. Тогда $Tor(G) = H$ и $G/Tor(G) \simeq Z^k$

Доказательство Так как все элементы H имеют конечный порядок, то $H \leq Tor(G)$. Покажем, что $Tor(G) \leq H$. Пусть $a \in Tor(G) \Rightarrow \exists n$ $na = 0$ и $n(a + H) = H \Rightarrow a + H \in Tor(G/H) \Rightarrow Tor(G)/H \leq Tor(G/H)$. Так как $G/H \simeq Z^k$, то $Tor(G/H) = \{e\}$ (в Z^k нет элементов конечного порядка). Значит, $Tor(G)/H = H$ и $Tor(G) + H = H$. По критерию принадлежности смежному классу, $Tor(G) \leq H$.

Тогда $Tor(G) = H$ и $G/Tor(G) = Z^k$

Замечание

В разложении конечнопорожденной абелевой группы G в прямую сумму циклических прямая сумма примарных циклических подгрупп и слагаемое Z^k определены однозначно с точностью до изоморфизма.

В частности, $k = rk(Z^k)$ определено однозначно.

Однако то, что разложение единственно пока еще не доказано.

Опр. **p-кручение** конечнопорожденной абелевой группы H — это множество $Tor_p(H) = \{a \in H \mid ord(a) = p^l$ для некоторого $l\}$, где p — простое число.

Утв.

Пусть $H = Z_{p_1^{\alpha_1}} \oplus ... \oplus Z_{p_s^{\alpha_s}}$ и все p_i простые (возможно, совпадающие). Тогда $Tor_p(H) \leq H$ и $Tor_p(H) = \oplus Z_{p_i^{\alpha_i}}$ — сумма по всем слагаемым, для которых $p_i = p$

Доказательство

$a_1, a_2 \in Tor_p(H) \Rightarrow \exists k_1, k_2 \in N$, что $p^{k_1} a_1 = p^{k_2} a_2 \Rightarrow ord(a_1 + a_2) | p^{k_1 + k_2}$ и $a_1 + a_2 \in Tor_p(H)$

Пусть $a \in H$, $a = (a_1, ..., a_s)$, $a_i \in Z_{p_i^{\alpha_i}}$. Если $ord(a) = \text{НОК}(ord(a_1), ..., ord(a_s))$ — степень числа p, то $ord(a_i) = 1$ для всех i, что $p_i \neq p$.

Значит, $Tor_p(H) = \oplus Z_{p_i^{\alpha_i}}$ по всем i, что $p_i = p$.

Следствие

В разложении конечнопорожденной абелевой группы в прямую сумму примарных циклических подгрупп сумма слагаемых, относящихся к одному простому числу p определяется однозначно, так как она есть p-кручение, независимое от разложения.

Осталось доказать, что если абелева группа разлагается в прямую сумму примарных циклических, относящихся к одному простому числу p, то все слагаемые определены однозначно.

Утв.

Пусть $H = Z_p^{\alpha_1} \oplus ... \oplus Z_p^{\alpha_s}$, p — простое. Тогда порядкислагаемых однозначно восстанавливаются по группе H с точностью до перестановки слагаемых.

Доказательство

Индукция по порядку группы H.

1. База: $H = \{e\}$ — верно, так как разложение пустое.

2. Переход: Пусть верно для всех групп порядка меньше, чем p^l. Тогда $pH = \{ph \mid h \in H\} \leq H$ и $pH = pZ_p^{\alpha_1} \oplus ... \oplus pZ_p^{\alpha_s} \simeq Z_p^{\alpha_1 - 1} \oplus ... \oplus Z_p^{\alpha_s - 1}$. Так как $H/pH = Z_p \oplus ... \oplus Z_p$ с тем же количеством слагаемых, то число слагаемых в исходной сумме определено однозначно.

   Применим предположение индукции к pH и получим, что набор ненулевых показателей определен однозначно (они же равны $\alpha_i - 1$.

   Но в силу того, что общее число слагаемых определено однозначно, то и число показателей, в которых $\alpha_i - 1 = 0$ так же определено однозначно.

   Таким образом, мы однозначно определили весь набор α_i.

Теорема (о единственности разложения конечнопорожденной абелевой группы в прямую сумму циклических

Пусть G — конечнопорожденная абелева группа. Тогда G допускает разложение $G = Z_{p_1^{\alpha_1}} \oplus ... \oplus Z_{p_s^{\alpha_s}} \oplus Z^k$, где p_i — простые (возможно, совпадающие) числа, а $s \in N$, возможно, нулевое.

Причем разложение единственно с точностью до перестановки слагаемых

Следствие

Если G — конечнопорожденная абелева группа и $Tor(G) = \{e\}$ ранга k, то $G \simeq Z^k$ для единственного k.

Так же, при $k \neq l$ $Z^k \neq Z_l$.

Теорема (об описании конечных подгрупп в мультипликативной группе поля

Пусть F — поле, $F^* = F \setminus \{0\}$ — мультипликативная группа поля. Тогда, если $G \leq F^*$ и $|G| \leq \infty$, то G — циклическая.

Доказательство

Очевидно, что G абелева и конечнопорождена. Тогда, $G = Z_{u_1} \times ... \times Z_{u_k}$, $u_i \geq 1$ и $u_1 | u_2 | ... | u_k$. $\forall a \in G$ верно $a^{u_k} = 1$, так как $u_k \,\vdots\, u_i$ $\forall i$. Значит, a — корень многочлена $x^{u_k} - 1$, а число корней многочлена не больше его степени, а значит $|G| \leq u_k$ и $|G| = u_1 ... u_k$, а значит $G \simeq Z_{u_k}$.

Следствие
Для конечного поля верно, что F^* — циклическая группа порядка $|F| - 1$.

2 Кольца и алгебры

Опр. **Кольцо** — множество R с определенными операциями сложения и умножения, где $(R, +)$ — абелева группа, $(R, *)$ — полугруппа (требуется только ассоциативность) и верна дистрибутивность $c(a+b) = ca + cb$, $(a+b)c = ac + bc$ $\forall a, b, c \in R$.

Если умножение коммутативно, то R — **коммутативное** кольцо (не абелево, так как этот термин применим только к группам).

Если в R есть нейтральный по умножению элемент, то он называется **единицей** и обозначается 1.

Опр. **Алгебра** — кольцо, являющееся линейным пространством над некоторым полем F и верно $\forall \alpha \in F$ $\forall a, b \in R$ $\alpha(ab) = (\alpha a)b = a(\alpha b)$

Примеры:

1. Если F — поле, то F — алгебра размерности 1 над самим собой.
2. $(Z, +, *)$ — кольцо
3. $F[x]$ — алгебра многочленов над полем F.
4. $(M_{n\times n}(F), +, *)$ — алгебра матриц над полем F.

Обе алгебры 3, 4 являются кольцами с единицей

Опр. **Подкольцо**(**подалгебра**) — непустое подмножество кольца (алгебры), само являющееся кольцом (алгеброй) относительно операций, определенных на исходной структуре.

Теорема (критерий подкольца)
$K \subset R$ — подкольцо $\Leftrightarrow$ K замкнуто относительно умножения и вычитания (сложения с обратным элементом по сложению).

Опр. Пусть R, S — кольца, тогда $\phi : R \to S$ — **гомоморфизм** колец (колец с единицей), если ϕ сохраняет операции сложения и умножения (для колец с единицей следует требовать $\phi(1_R) = 1_S$, так как это не следует из определения гомоморфизма колец)
$Im(\phi) = \{\phi(a) \mid a \in R\}$
$Ker(\phi) = \{a \in R \mid \phi(a) = 0_S\}$

Примеры:

1. $\phi : Z \to Z_n,\ \phi(a) = a + nZ$ — гомоморфизм колец с единицей, так как $\phi(1) = 1 + nZ = 1_{Z_n}$
2. R — алгебра матриц $M_{n\times n}(F)$, S — алгебра матриц $M_{k\times k}(F)$, $\phi(A) = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ — гомоморфизм алгебр (без единицы, так как $\phi(1_R) \neq 1_S$.

Опр. Пусть R — кольцо. Полукольцо I — **левый (правый) идеал** в R, если $\forall x \in R$ $\forall a \in I$ верно $xa \in I$ $(ax \in I)$, то есть левый (правый) идеал выдерживает умножение слева (справа) на элементы кольца.

Если идеал двусторонний, то он называется просто идеалом

Утв.
Пусть $\phi : R \to S$ — гомоморфизм колец. Тогда $Im(\phi) S$ (подкольцо) и $Ker(\phi) \triangleleft R$ (идеал)

Доказательство
$\phi : (R, +) \to (S, +)$ — гомоморфизм групп, значит $Im(\phi) \leq S$ — подгруппа. Проверим замкнутость относительно умножения: $\phi(a)\phi(b) = \phi(ab) \in Im(\phi)$.

Известно, что $Ker(\phi) \triangleleft (R, +)$ — нормальная подгруппа. Пусть $a \in Ker(\phi)$, $x \in R$. Тогда $\phi(ax) = \phi(xa) = 0$, так как $\phi(a) = 0$, то есть $ax, xa \in Ker(\phi)$ и $Ker(\phi)$ — идеал

3 Факторкольцо по идеалу

Пусть R — кольцо и I — его идеал.

Опр. **Факторкольцо по идеалу** — факторгруппа $(R, +)$ по $(I, +)$ $R/I = \{x + I \mid x \in R\}$ с определенной операцией умножения $(x + I)(y + I) = xy + I \in R/I$.

Данное определение корректно. Пусть $x + I = x' + I$ и $y + I = y' + I$. Тогда $x' = x + a$ и $y' = y + b$, $a, b \in I$ и $(x' + I)(y' + I) = x'y' + I = (x + a)(y + b) + I = xy + ay + xb + ab + I = xy + I$, так как I — идеал.

Теорема
Множество смежных классов по идеалу I — кольцо относительно операций $(x + I) + (y + I) = (x + y) + I$ и определенной выше операции умножения.

Отображение $p : R \to R/I$ $p(x) = x + I$ — эпиморфизм (сюръективный гомоморфизм) колец.

Доказательство
$p(x + y) = x + y + I = p(x) + p(y)$
$p(xy) = xy + I = (x + I)(y + I) = p(x)p(y)$
p сюръективен для групп, а значит и для колец. Образ кольца при гомоморфизме есть кольцо, а значит R/I — кольцо

Опр. Построенное кольцо — **факторкольцо** R по идеалу I. p — **канонический эпиморфизм**.

Теорема (о гомоморфизмах колец)
Пусть $\phi : R \to S$ — гомоморфизм колец. Тогда $Im(\phi) \leq S$ и $Ker(\phi) \triangleleft R$ и $Im(\phi) \simeq R/Ker(\phi)$, причем существует такой изоморфизм $\psi : Im(\phi) \to R/Ker(\phi)$, что $\psi \circ \phi = p$, где p — канонический эпиморфизм.

Доказательство
$\phi : (R, +) \to (S, +)$ — гомоморфизм групп. Для соответствующих групп верна теорема о гомоморфизме групп: $Im(\phi) \simeq R/Ker(\phi)$. Обозначим этот изоморфизм $\psi : Im(\phi) \to R/Ker(\phi)$. Этот гомоморфизм групп сохраняет операцию умножения, так как по определению $\psi(x)$ есть полный прообраз x, а это есть смежный класс $a + Ker(\phi)$, где a — произвольный элемент R, что $\phi(a) = x$.

Тогда $\psi(xy) = (ab + Ker(\phi) = (a + Ker(\phi))(b + Ker(\phi)) = \psi(x)\psi(y)$.