Конспект вопросов по компьютерной алгебре. Первый семестр. 2010.

Преподаватель: Васильев Николай Николаевич

Содержание

1 Группа, подгруппа, гомоморфизм групп. Ядро и образ гомоморфизма.

Определение. $< G, *, e >$ - группа, $* : G \times G \to G, e \in G$

1. $\forall a, b, c \in G\ (ab)c = a(bc)$
2. $\forall g \in G\ eg = ge = g$
3. $\forall g \in G\ \exists g^{-1} \in G\ gg^{-1} = g^{-1}g = e$

Если $\forall a, b \in G\ ab = ba$ то группу называют *абелевой*

Теорема. $\exists! e \in G\ eg = ge = g$

Определение. G - группа, тогда $H \subset G$ называют *подгруппой*, если

1. $e \in H$
2. $\forall h_1, h_2 \in H\ h_1h_2 \in H \mid HH \subset H$
3. $\forall h \in H\ h^{-1} \in H \mid H^{-1} \subset H$

Определение. G, W - группы.
$f : G \to W$ называют *гомоморфизмом (групп)*, если $\forall g_1, g_2 \in G\ f(g_1g_2) = f(g_1) * f(g_2)$

Теорема. *$f : G \to W$ - гомоморфизм*
$f(e_G) = e_W$

Определение. $f : G \to W$ - гомоморфизм, тогда
$kerf = g \in G|f(g) = e_W$ - называют *ядром гомоморфизма f*

Теорема. *$kerf$ - подгруппа G*

Определение. $f : G \to W$ - гомоморфизм, тогда
$Imf = \{w \in W|\exists g \in G\ f(g) = w\}$ - называют *образом гомоморфизма f*

2 Мономорфизмы, эпиморфизмы и изоморфизмы. Понятие нормального делителя (нормальной подгруппы). Факторгруппа.

Определение. Сюръективный гомоморфизм - *эпиморфизм.*
Инъективный гомоморфизм - *мономорфизм.*
Биективный гомоморфизм - *изоморфизм.*
Изоморфизм $f : G \to G$ - *автоморфизм.*

Пусть $H \subset G$. Введем отношение эквивалентности $\sim$ соответствующее подгруппе. $g_1, g_2 \in G$. $g_1 \sim g_2$, если $g_1 g_2^{-1} \in H$

Определение. $\widetilde{g} = \{k \in G | k \sim g\}$ - *класс эквивалентности элемента* g

Определение. G/H - *факторгруппа, левые смежные классы.* $\widetilde{g} = Hg$

Заметим, что в случае некоммутативной группы можно ввести правые смежные классы gH.

Теорема. *Если $gH = Hg$, то G/H - группа.*

Доказательство. Введем умножение: $\forall g_1 H, g_2 H \in G/H$ $(g_1 H)(g_2 H) \overset{def}{=} g_1 g_2 H$.
Проверим корректность умножения: пусть $g_1' \sim g_1, g_2' \sim g_2$. Тогда $g_1' = g_1 h_1, g_2' = g_2 h_2$, а значит $g_1' g_2' = g_1 h_1 g_2 h_2 = g_1 g_2 h_1 h_2$. То есть $g_1' g_2' H = g_1 g_2 H$.
Теперь проверим свойства умножения:

1. $eHgH = gH$
2. $g_1 H g_2 H g_3 H = g_1 g_2 g_3 H$
3. $gHg^{-1}H = eH$

□

Определение. $H \subset G$ назовем *нормальной подгруппой*, если $\forall g \in G$ $gH = Hg$ или $gHg^{-1} = H$ или $ghg^{-1} \in H$
Обозначение: $H \triangleleft G$

Теорема. *G - абелева группа, тогда $\forall H \subset G$ - нормальная.*

Теорема. *Ядра гомоморфизмов и только они суть нормальные подгруппы.*

Доказательство. Сперва докажем, что если $f : G \to W$ - гомоморфизм, то $ker f \triangleleft G$. $g \in G, h \in ker f$, тогда $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(g)^{-1} = e_W$.
Теперь покажем, что $\forall H \triangleleft G\ \exists f$ - гомоморфизм и $ker f = H$. Введем $\pi_H : G \to G/H$ - канонической гомоморфизм. Пусть $g \in G, h \in H$ тогда $\pi_H(g) = gH, \pi_H(h) = hH = H$. Следовательно $ker \pi_H = H$. $\square$

Порой пишут: $\{e\} \subset H \triangleleft G \xrightarrow{\pi_H} G/H$

3 Характеризация мономорфизмов в терминах ядра. Основная теорема о гомоморфизме.

Теорема. *ϕ - мономорфизм $\Leftrightarrow ker\phi = \{e\}$*

Доказательство. [$\Rightarrow$] Пусть $\exists g \neq e \ \phi(g) = e$. Но $\phi(e) = e$. Таким образом $g \neq e, \phi(g) = \phi(e)$. Противоречие инъективности.
[$\Leftarrow$] Пусть $\exists g_1 \neq g_2, \phi(g_1) = \phi(g_2)$. Тогда $\phi(g_1)\phi(g_2)^{-1} = e$, а это значит, что $g_1g_2^{-1} \neq e$ и $g_1g_2^{-1} \in kerf$. Противоречие тривиальности ядра. □

Теорема. *$G/kerf \cong Imf$*

Доказательство. Пусть $\phi : X \leftarrow Y$. Введем отношение эквивалентности: $x_1 \sim x_2$, если $\phi(x_1) = \phi(x_2)$. Рассмотрим $\tau : X/\sim \ \rightarrow Im\,\phi$, $\tau(\widetilde{x}) = \phi(x)$.
τ - инъекция. Действительно, если $\widetilde{x_1} \neq \widetilde{x_2}$, то x_1 не эквивалентно x_2 и значит $\phi(x_1) \neq \phi(x_2)$.
τ - сюръекция. Действительно $\forall y \in Im\,\phi \ \exists x \ \phi(x) = y$ и $\widetilde{x} : \tau(\widetilde{x}) = y$. Таким образом изоморфизм установлен.
Теперь пусть $f : G \rightarrow W$ - гомоморфизм. $g_1 \sim g_2$, если $f(g_1) = f(g_2)$, или $f(g_1)f(g_2)^{-1} = e, f(g_1g_2^{-1}) = e$ это означает, что $g_1g_2^{-1} \in kerf$. То есть отношение $\sim$ совпадает с отношением эквивалентности порождаемым $kerf \lhd G$. Можно записать $G/kerf \cong Imf$. □

4 Группа подстановок (симметрическая группа). Четные и нечетные подстановки. Теорема о том, что всякая группа есть подгруппа симметричской группы (для конечных групп).

Определение. *Симметрической группой* S_X множества X называется группа автоморфизмов $X \to X$ относительно операции композиции и нейтрального элемента $id_X : \forall x \in X, id_X(x) = x$.
Если $X = \{1, 2, \cdots, n\}$, то симметричскую группу называют группой подстановок и обозначают S_n.

Группа подстановок S_n допускает следующее копредставление:

Образующие:
$\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$

Соотношения:
$\sigma_i^2 = 1$
$\sigma_i \sigma_j = \sigma_j \sigma_i$, если $|i - j| > 1$
$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$

Вообще, образующие в указанном копредставлении являются *транспозициями*, то есть это такие подстановки, которые меняют два соседних элемента местами, а остальные элементы оставляют на месте.

Определение. Подстановка называется *четной*, если она представляется в виде произведения четного числа транспозиций и *нечетной* в противном случае.

Теорема. *Любая группа - подгруппа симметрической группы.*

Доказательство. Необходимо сопоставить каждому элементу $g \in G$ некоторую биекцию $G \to G$, тем самым получив вложение $G \subset S_G$. Рассмотрим $i_g : G \to G, \forall s \in G\ i_G(s) = gs$. Осталось проверить свойства: $i_a \circ i_b = a(bs) = (ab)s = i_{ab},\ i_g \circ i_{g^{-1}} = g(g^{-1}s) = es = i_e$. □

5 Левые классы смежности по подгруппе (см. вопрос 2). Индекс подгруппы. Теорема об индексе.

Определение. $H \subset G$
$[G : H] = \#G/H$ - *индекс* подгруппы.
$\#G$ - *порядок, мощность* группы.

Замечание: индекс тривиальной подгруппы - порядок группы.

Теорема (Теорема об индексе)**.** *$K \subset H \subset G$,*
тогда $[G : K] = [G : H][H : K]$

Доказательство. $G = \bigcup\limits_{i=1}^{[G:H]} g_i H$ при этом $g_i H \neq g_j H, i \neq j$. Аналогично $H = \bigcup\limits_{j=1}^{[H:K]} h_j K$ при этом $h_i K \neq h_j K, i \neq j$. Запишем $G = \bigcup\limits_{i,j} g_i h_j K$.
Теперь достаточно проверить, что $g_i h_j K$ представляют все различные классы смежности по K. Пусть $g_i h_j K = g_l h_m K$. Умножим на H, получим $g_i h_j KH = g_l h_m KH$, и далее $g_i h_j H = g_l h_m H \Rightarrow g_i H = g_l H \Rightarrow i = l$. Вернемся к исходному равенству $g_i h_j K = g_i h_m K \Rightarrow h_j K = h_m K \Rightarrow j = m$. То есть все классы различны.
Возьмем gK. Ясно, что $g = g_i h, h \in H$ и $h = h_m k, k \in K$. Имеем $g = g_i h_m k, g \in g_i h_m K$. Теперь понятно, что исходное представление G представляло все классы смежности по K. $\square$

Следствия:

1. Порядок подгруппы всегда делитель порядка группы.
   Пусть $K = \{e\}$, по теореме об индексе $\#G = \#(G/H)\#H$

2. $\forall G : \#G = p, p \in \mathbb{P}$ - циклическая группа порядка p
   Рассмотрим $G : \#G = p, p \in \mathbb{P}$. Рассмотрим $H \subset G$ - циклическая подгруппа, порожденная $g \neq e$. Ясно, что $\#H \geq 2$. Но $\#H$ делитель $\#G = p$, а значит $\#H = p = \#G$. Также из этого следует $\forall G : \#G = p, p \in \mathbb{P} \quad G \cong \mathbb{Z}/p\mathbb{Z}$

6 Свободная группа. Теорема о том, что всякая группа есть факторгруппа свободной группы.

Пусть $S = \{a, b, c \cdots\}$, $S^{-1} = \{a^{-1}, b^{-1}, c^{-1}, \cdots\}$. Будем называть $A = S \cup S^{-1}$ *алфавитом*, а A^* - множеством всевозможных слов над алфавитом A. *Пустым* словом будем называть $aa^{-1} = \emptyset$. Введем отношение эквивалентности на A^*. $w \sim v$, если w можно получить из v с помощью правил сокращения. Также введем операцию *конкатенации* на A^*.

Определение. $F_S = A^* \cup \emptyset / \sim$ - группа по конкатенации. F_S - *свободная группа*, порожденная S.

Теорема (Категорное свойство свободной группы)**.** *Существует единственный гомоморфизм, делающий диаграмму коммутативной. То есть* $\forall f : S \to G \;\; \exists! \phi_f : F_S \to G, \;\; f = \phi_f \circ i.$

$$\begin{tikzcd} & F_S \arrow[dd, dashed, "\varphi_f"] \\ S \arrow[ur, "i"] \arrow[dr, "f"'] & \\ & G \end{tikzcd}$$

Доказательство. Пусть $S = \{s_1, \cdots, s_n\}$. Тогда $Imf = \{f(s_1, \cdots, f(s_n)\} = \{g_1, \cdots, g_n\}$. Теперь введем $\phi_f(s_1^{n_1} s_2^{n_2} \cdots s_i^{n_i}) = g_2^{n_1} g_2^{n_2} \cdots g_i^{n_i}$. Единственность очевидна по построению. □

Теорема. *Приведенное выше свойство может быть принято за определение свободной группы с точностью до изоморфизма.*

Доказательство. Пусть существуют две свободные группы, порожденные $S : F_1$ и F_2. Тогда по свойству существуют единственные гомоморфизмы $\phi_i : F_1 \to F_2$ и $\phi_j : F_2 \to F_1$. А это значит, что $F_1 \overset{\sim}{=} F_2$.

$$\begin{tikzcd} & F_1 \arrow[dd, dashed, shift left, "\varphi_i"] \\ S \arrow[ur, "i"] \arrow[dr, "j"'] & \\ & F_2 \arrow[uu, dashed, shift left, "\varphi_j"] \end{tikzcd}$$

□

Теорема. *Любая группа есть факторгруппа некоторой свободной группы.*

Доказательство. Пусть G - группа. Забудем о её груповых свойствах и рассмотрим как множество. Рассмотрим F_G - свободную группу, порожденную G. Теперь вспомним о том, что G - группа. Тогда $\exists \phi : F_G \to G$ - естественный эпиморфизм групп, то есть $Im\, \phi = G$. По основной теореме о гомоморфизме $F_G/ker\phi \cong Im\, \phi = G$. □

Пример:
$F_{\{a,b\}} \cong \mathbb{Z}\times\mathbb{Z}$, если введены следующие правила $aba^{-1}b^{-1} = e, ab = ba$.