Лекция 2, 30.09.11

Элемент e некоторой полугруппы называется *идемпотентом*, если $e^2 = e$.

Лемма 1. *В конечной полугруппе для любого элемента найдется его степень, которая является идемпотентом.*

Доказательство. Пусть S – конечная полугруппа, $a \in S$. Рассмотрим последовательность степеней $a, a^2, a^3, \ldots$. Поскольку последовательность бесконечна, а полугруппа конечна, найдутся такие натуральные числа n и k, что $a^n = a^{n+k}$. Понятно, что тогда $a^m = a^{m+k}$ для любого $m \geq n$. Рассмотрим элемент a^{nk}. Имеем

$$a^{nk} = a^{nk+k} = a^{nk+2k} = \cdots = a^{nk+nk} = (a^{nk})^2.$$

Следовательно, a^{nk} – идемпотент. □

Упражнение 1. *Пусть полугруппа S имеет порядок n. Доказать, что для любого $a \in S$ элемент $a^{n!}$ – идемпотент.*

Предложение 1. *В конечной полугруппе $\mathscr{D} = \mathscr{J}$*

Доказательство. Включение $\mathscr{D} \subseteq \mathscr{J}$ выполняется в силу того, что $\mathscr{J}$ содержит $\mathscr{L}$ и $\mathscr{R}$, а $\mathscr{D}$ – наименьшее отношение эквивалентности, содержащее и $\mathscr{L}$, и $\mathscr{R}$.

Пусть $a \mathscr{J} b$. Найдутся такие $u, v, x, y \in S^1$, что $uav = b$ и $xby = a$, откуда $xuavy = a$. Подставляя в левую часть этого равенства $xuavy$ вместо a, получим $(xu)^2 a (vy)^2 = a$. Повторяя этот процесс, получим, что $(xu)^k a (vy)^k = a$ для любого k. По лемме 1 найдется такое k, что элементы $e = (xu)^k$ и $f = (vy)^k$ – идемпотенты. Равенство $(xu)^k a (vy)^k = a$ можно переписать как $eaf = a$. Домножая его слева на e, получим $eaf = ea$, откуда $ea = a$. Аналогично, домножая равенство $eaf = a$ справа на f, получим $eaf = af$, откуда $af = a$.

Покажем, что $ua \mathscr{L} a$. Ясно, что $ua \in S^1 a$. Обратно, имеем $a = ea = (xu)^k a = (xu)^{k-1} x \cdot ua \in S^1 ua$. Аналогично проверяется, что $a \mathscr{R} av$. Учитывая, что отношение $\mathscr{R}$ стабильно справа, получаем, что $ua \mathscr{R} uav = b$. Итак, $a \mathscr{L} ua \mathscr{R} b$, т. е. $a \mathscr{L}\mathscr{R} b$ и $a \mathscr{D} b$ □

Предложение 2.

1. *Пусть e – идемпотент. Тогда $a \leq_{\mathscr{R}} e$ тогда и только тогда, когда $ea = a$, и $a \leq_{\mathscr{L}} e$ тогда и только тогда, когда $ae = a$.*

2. *Если $a \leq_{\mathscr{R}} axy$, то $a \mathscr{R} ax \mathscr{R} axy$. Если $a \leq_{\mathscr{L}} yxa$, то $a \mathscr{L} xa \mathscr{L} yxa$.*

В конечных полугруппах верны еще два свойства.

3. Если $a \leq_{\mathscr{J}} ax$, то $a \mathscr{R} ax$. Если $a \leq_{\mathscr{J}} xa$, то $a \mathscr{L} xa$.

4. Если $a \leq_{\mathscr{L}} b$ и $a \mathscr{J} b$, то $a \mathscr{L} b$. Если $a \leq_{\mathscr{R}} b$ и $a \mathscr{J} b$, то $a \mathscr{R} b$.

Доказательство. 1. Если $a \leq_{\mathscr{R}} e$, то найдется такой элемент $u \in S^1$, что $a = eu$. Умножив это равенство на e слева, получим $ea = eu = a$. Обратная импликация очевидна.

2. Ясно, что $a \geq_{\mathscr{R}} ax \geq_{\mathscr{R}} axy$. Поэтому если $a \leq_{\mathscr{R}} axy$, то $a \mathscr{R} ax \mathscr{R} axy$.

3. Если $a \leq_{\mathscr{J}} ax$, то найдутся такие элементы $u, v \in S^1$, что $a = uaxv$. Подставляя в правую часть этого равенства $uaxv$ вместо a, получим, что $a = u^k a(xv)^k$ для всех натуральных k. По лемме 1 найдется такое k, что $u^k = e$ – идемпотент. Тогда $a = ea(xv)^k$, откуда $a = ea$ и $a = a(xv)^k = ax \cdot v(xv)^{k-1}$. Мы видим, что $a \leq_{\mathscr{R}} ax$. Поскольку всегда выполняется $a \geq_{\mathscr{R}} ax$, заключаем, что $a \mathscr{R} ax$.

4. Если $a \leq_{\mathscr{L}} b$, то $a = ub$ для некоторого $u \in S^1$. Поэтому $ub \mathscr{J} b$, откуда по предыдущему пункту имеем $b \mathscr{L} ub$, т. е. $a \mathscr{L} b$. □

Пусть $a \in S$, договоримся обозначать

$\mathscr{R}$-класс, содержащий a, через R_a;
$\mathscr{L}$-класс, содержащий a, через L_a;
$\mathscr{H}$-класс, содержащий a, через H_a;
$\mathscr{D}$-класс, содержащий a, через D_a.

Заметим, что $H_a = L_a \cap R_a$ для любого a.

Лемма 2. *Пусть L – $\mathscr{L}$-класс, R – $\mathscr{R}$-класс. Тогда $R \cap L \neq \varnothing$ тогда и только тогда, когда L и R содержатся в одном D-классе.*

Доказательство. Пусть $a \in L \cap R$. Тогда ясно, что L и R содержатся в D_a.

Обратно, пусть L и R содержатся в $\mathscr{D}$-классе D. Возьмем произвольные $x \in L$ и $y \in R$. Тогда $x \mathscr{D} y$, т. е. существует такой элемент a, что $x \mathscr{L} a \mathscr{R} y$. Тогда $a \in L \cap R$, откуда $L \cap R \neq \varnothing$. □

Лемма 2 подсказывает, что $\mathscr{D}$-классы удобно мыслить себе как прямоугольные таблицы (по традиции именуемые *egg-box картинками*), в которых строки изображают $\mathscr{R}$-классы, столбцы – $\mathscr{L}$-классы, а ячейки – $\mathscr{H}$-классы.

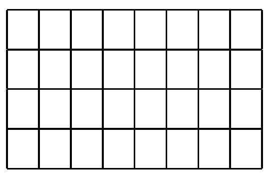

Рис. 1: Egg-box картинка

Следующий важный результат показывает, что элементы каждого $\mathscr{D}$-класса распределены по ячейкам соответствующей egg-box картинки равномерно.

Предложение 3 (Лемма Грина). *Пусть $a\mathscr{R}b$, т. е. существуют $u, v \in S^1$, такие что $au = b$ и $bv = a$. Рассмотрим отображения $\rho_u : S \to S$, задаваемое правилом $x\rho u = xu$, и $\rho_u : S \to S$, задаваемое правилом $x\rho v = xv$. Тогда ограничение ρ_u на класс L_a – это биекция L_a на L_b, ограничение ρ_v на класс L_b – обратная к ней биекция, и оба ограничения сохраняют $\mathscr{H}$-классы.*

Доказательство. Возьмем произвольный элемент $x \in L_a$. Из $x \mathscr{L} a$ следует, что $xu \mathscr{L} au = b$, поскольку отношение $\mathscr{L}$ стабильно справа. Следовательно, $L_a\rho_u \subseteq L_b$. Далее, существует элемент $t \in S^1$, такой, что $x = ta$. Имеем

$$x\rho_u\rho_v = xuv = tauv = tbv = ta = x,$$

т. е. ограничение ρ_v на класс L_b – обратное отображение к ограничению ρ_u на класс L_a.

Получается, что ограничение ρ_v на класс L_b отображает L_b на L_a, следовательно, ограничения ρ_u и ρ_v на соответственно L_a на L_b – взаимно обратные биекции. Поскольку $xuv = x$, имеем $x\mathscr{R}xu$, и если $x \mathscr{H} y$, то $xu \mathscr{H} yu$. Обратно, если $xu \mathscr{H} yu$, то $x \mathscr{H} y$ □

Предложение 4 (Теорема Миллера-Клиффорда). *Пусть $a, b \in S$, тогда $ab \in R_a \cap L_b$ тогда и только тогда, когда пересечение $R_b \cap L_a$ содержит идемпотент.*

Доказательство. Пусть $ab \in R_a \cap L_b$. По лемме Грина $\rho_b|_{L_a}$ – биекция L_a на L_b. Поэтому в $R_b \cap L_a$ найдется такой элемент e, что $e\rho_b = eb = b$. Поскольку $e\mathscr{R}b$, имеем $e = bx$ для некоторого $x \in S^1$. Отсюда $e^2 = e(bx) = (eb)x = bx = e$, т. е. e – идемпотент.

Обратно, пусть e – идемпотент из $R_b \cap L_a$. Имеем $eb = b$ и $ae = a$. Умножив отношение $e\mathscr{R}b$ слева на a, получим $a = ae, \mathscr{R} ab$. Аналогично, умножив отношение $e\mathscr{L}a$ справа на b, получим $b = eb\mathscr{L}ab$. Следовательно $ab \in R_a \cap L_b$. □

Следствие 1. *Пусть H — $\mathscr{H}$-класс, тогда следующие условия эквивалентны:*

1. *H содержит идемпотент.*
2. *Существуют $a, b \in H$, такие, что $ab \in H$.*
3. *H – группа.*

Доказательство. Импликации $1 \Rightarrow 2$ и $3 \Rightarrow 1$ очевидны.

$2 \Rightarrow 3$. Имеем $H = R_a \cap L_b = R_b \cap L_a$. По теореме Миллера-Клиффорда в H найдется идемпотент e. Применяя ту же теорему в обратную сторону, заключаем, что для любых $g, h \in H$ произведение gh принадлежит H, т. е. H – полугруппа. Для любого $h \in H$ отображение $\rho_h|_H$ – биекция H на H. Отсюда, в частности, следует, что $ge = g$ для любого $g \in H$. В силу симметричных рассуждений $eg = g$ для любого $g \in H$, т. е. e – единица в H. Наконец, из того, что $\rho_h|_H$ – биекция H на H, следует, что для любого $h \in H$ существует элемент h', такой, что $h'h = e$. Следовательно H – группа. □

Заметим, что если H – группа, то H – максимальная подгруппа. Действительно, если G – какая-то подгруппа полугруппы S, то любые два элемента $g, h \in G$ делят друг друга и справа, и слева: $g = h \cdot h^{-1} g$, $h = g \cdot g^{-1} h$ и аналогично слева. Поэтому G содержится в некотором $\mathscr{H}$-классе H. Поскольку H содержит идемпотент (а именно, единицу подгруппы G), по только что доказанному следствию H есть подгруппа. Итак, каждая подгруппа полугруппы содержится ровно в одной максимальной подгруппе, а именно, в $\mathscr{H}$-классе единицы этой подгруппы.