Список литературы

1. Левашев Е.А. Дис. ... д-ра техн. наук/ МГИСИС. – М., 1995. – 97с.
2. Котин И.М. Вестник Полоцкого государственного университета. Серия С: Фундаментальные науки. Физика, 2011, №4. – С.97–105.
3. Merzhanov A.G., Rogachev A.S., Sytschev A.E. et al. Proceeding of the 1st Sino-Russian workshop on SHS. Beijing. China. 2000. – P. 133–140.

ТОЖДЕСТВА НА ПОЛУГРУППАХ ЛИНЕЙНЫХ ОТНОШЕНИЙ

М.И. Наумик

Витебск, УО «ВГУ им. П.М. Машерова»

Напомним, что полугруппа называется идемпотентной, если она удовлетворяет тождеству $a^2 = a$. Как известно, на каждой идемпотентной полугруппе отношение $a \le b$, вводимое посредством условия $ab = ba = a$, определяет порядок. Очевидно, что идемпотентная полугруппа коммутативна тогда и только тогда когда соответствующее упорядоченное множество является нижней полурешеткой. Еще один важный класс составляют полугруппы идемпотентов, порядок на которых совпадает с равенством. Это в точности вполне простые полугруппы идемпотентов. Они называются прямоугольными. Частыми случаями прямоугольных являются сингуляторные полугруппы, – правосингуляторные (или полугруппы правых нулей) и левосингуляторные (или полугруппы левых нулей).

Перейдем к рассмотрению идемпотентных полугрупп линейных отношений. Пусть V – левое n-мерное векторное пространство над произвольным телом F. Бинарное отношение $a \le V \times V$ между элементами множества V называется линейным, если оно является подпространством $V \oplus V$. Другими словами, линейное отношение a – это множество пар $(\bar{x};\bar{y})$, где $(\bar{x};\bar{y}) \in V$, замкнутое относительно операций сложения и умножения на элемент из F: если $(\bar{x}_1;\bar{y}_1) \in a$ и $(\bar{x}_2;\bar{y}_2) \in a$ при каких-либо $\bar{x}_i, \bar{y}_i \in V$, то $(\alpha\bar{x}_1 + \beta\bar{x}_2; \alpha\bar{y}_1 + \beta\bar{y}_2) \in a$ для любых $\alpha, \beta \in F$.

Множество $LR(V)$ всех линейных отношений на пространстве V является, как известно, полугруппой относительно операции умножения бинарных отношений.

При изучении линейных отношений $a \in LR(V)$ будем рассматривать следующие подпространства пространства V:

$$pr_1 a = \{\bar{x} \in V : \exists \bar{y} \in V, (\bar{x};\bar{y}) \in a\}; \quad \ker a = \{\bar{x} \in V : (\bar{x};\bar{o}) \in a\};$$

$$pr_2 a = \{\bar{y} \in V : \exists \bar{y} \in V, (\bar{x};\bar{y}) \in a\}; \quad co\ker a = \{\bar{y} \in V : (\bar{o};\bar{y}) \in a\}.$$

Все другие определения и обозначения можно найти в [1, 2, 3].

Пусть $\Gamma \subseteq LR(V)$ подполугруппа полугруппы $LR(V)$. Обозначим

$$\ker\Gamma = \bigcap_{a\in\Gamma} \ker a, \quad pr_2\Gamma = \sum_{a\in\Gamma} pr_2 a, \; pr_1\Gamma = \bigcap_{a\in\Gamma} pr_1 a, \tag{1}$$

$$\mathrm{Coker}\Gamma = V/pr_2\Gamma \tag{2}$$

Отметим, что если a – *идемпотент из* $LR(V)$, то существует такое пространство V_1, что $pr_1 a = \ker a \oplus V_1$, $pr_2 a = co\ker a \oplus V_1$ и для любого $\bar{x} \in V_1$ имеем $(\bar{x};\bar{x}) \in a$.

Полугруппу из $LR(V)$ будем называть линейной полугруппой степени n.

Обозначим через L^0 полное подпространство пространства U^* (U^* сопряженное к U), ортогональное к подпространству L пространства V. Поставим в соответствие каждому Г– бимодулю V аналогичный ^{t}Г– бимодуль ^tV следующим образом:

$$^t(L/M)=M^0/L^0$$

$$^t(V_1\times V_2\times\ldots V_m)={}^tV_1\times\ldots\times{}^tV_m \tag{3}$$

Отметим очевидное соотношение $\ker{}^ta=(pr_2a)^0$ для линейного отношения a.

Из (1), (2), (3) и указанного соотношения вытекают следующие равенства:

$$\ker{}^t\Gamma=(pr_2\Gamma)^0 \tag{4}$$

$$^t(Co\ker\Gamma)=\ker{}^t\Gamma,\ {}^t(Coim\Gamma)=pr_2\ {}^t\Gamma \tag{5}$$

Пусть V_1 и V_2 – пространства над одним телом, $\Gamma\subseteq LR(V_1)$ и $\Delta\subseteq LR(V_2)$. Если существует отображение $f:a\to a'$ множества Г на множество Δ и такой изоморфизм θ пространства V_1 на пространство V_2, что $a\circ\theta=\theta\circ a'$ для всех $a\in\Gamma$, то будем называть множества Г и Δ подобными (относительно изоморфизма θ).

Значительная часть приложений двойственности базируется на теореме, интуитивная ясность которой не избавляет от формальных трудностей ее доказательства.

Теорема 1. Пусть даны векторное пространство V_1, множество $\Gamma\subset LR(V_1)$ и Г – бимодуль V_2. Тогда множество $^t(\Gamma[V_2])$ и $^t(\Gamma[{}^tV_2])$ канонически подобны.

Впредь мы будем отождествлять канонически подобные множества линейных отношений.

Введем обозначение и терминологию, связанные с тождествами на полугруппах. Зафиксируем счетный алфавит

$$X\{x, y, x_1, x_2, \ldots, x_n, \ldots\}.$$

Если W – слово в алфавите X, то $C(W)$ будем обозначать множество всех букв из X, входящих в W. Пусть Г – произвольная полугруппа, $C(W)\subseteq У\subseteq X$ и $f: У\to\Gamma$ – некоторое отображение. Посредством W^f обозначим элемент в Г, соответствующий слову W при отображении f.

Как обычно будем говорить, что тождество $W_1 = W_2$, где W_1, W_2 –непустые слова, выполняются в полугруппе Г и писать $\Gamma\models W_1 = W_2$, если $W_1^f=W_2^f$ для любого отображения $f: C(W_1W_2)\to\Gamma$.

Через $\overline{W}$ обозначим слово, полученное из слов W инверсированием, т.е. перестановкой всех букв в обратном порядке. Если Г – линейная полугруппа, то, как легко видеть, из $\Gamma\models W_1 = W_2$ вытекает $^t\Gamma\models\overline{W_1}=\overline{W_2}$.

Теорема 2. Пусть $\Gamma\subseteq LR(V)$ – полугруппа, W_1 и W_2 – непустые слова и $x\notin C(W_1W_2)$. Если $\Gamma\models W_1x=W_2x$, то $\Gamma[Coim\Gamma]\models W_1=W_2$.

Доказательство. Положим $\Gamma_1=[Coim\Gamma]$, $У = C(W_1W_2)$. Возьмем какое-нибудь отображение $f: У\to\Gamma_1$, канонический эпиморфизм $\varepsilon: pr_1\Gamma_1\to Coim\Gamma$, а также индуцированный им полугрупповой гомоморфизм η $:\Gamma\to\Gamma_1$. Рассмотрим произвольное отображение $g:\text{У}\cup\{x\}\to\Gamma$, ограничение которого на *У* (обозначим его тоже буквой *g*) удовлетворяет равенству $g\circ\eta = f$. Пусть $x^g = a$. Тогда, так как Γ ⊨ $W_1x = W_2x$, для любого $u\in pr_1\Gamma$ имеем $(u,u_1)\in W_1^g a$ и $(u,u_1)\in W_2^g a$ или $(u,u_2)\in W_1^g$, $(u_2,u_1)\in a$, $(u,u_3)\in W_2^g$, $(u_3,u_1)\in a$, т.е. $u_2-u_3\in\ker a$. Поскольку $x\notin\text{У}$, в качестве *a* можно брать любой элемент из Γ, откуда $u_2-u_3\in\bigcap\limits_{a\in\Gamma}\ker a=\ker\Gamma$. Факторизуя *V* по ker Γ и учитывая, что для слова *W* в алфавите *У* выполняется (по определению *g*) равенство $W^g\eta=W^f$, получим для любого $\upsilon\in Coim\Gamma$ справедливо равенство $\upsilon W_1^f=\upsilon W_2^f$. Ввиду произвольности отображения *f* теорема доказана.

Следствие. Пусть $\Gamma\subseteq LR(V)$ – полугруппа, W_1 W_2 – непустые слова и $x\notin C(W_1W_2)$. Если $\Gamma\models xW_1 = xW_2$, $\Gamma[\ker\Gamma + pr_2\Gamma]\models W_1 = W_2$.

Теорема 3. Пусть $\Gamma\subseteq LR(V)$ – полугруппа, W_1 и W_2 – непустые слова и $x\notin C(W_1W_2)$. Если $\Gamma\models xW_1 = xW_2$, то $\Gamma[pr_2\Gamma]\models W_1 = W_2$.

Доказательство. Пусть на Γ выполняется тождество $xW_1 = xW_2$.

Тогда ${}^t\Gamma\models\overline{W_1}x=\overline{W_2}x$ и, по теореме 2, ${}^t\Gamma[Coim\,{}^t\Gamma]\models\overline{W_1}=\overline{W_2}$. Но из теоремы 1 и второго равенства (5) следует, что

${}^t\Gamma[Coim\,{}^t\Gamma]={}^t(\Gamma[{}^tCoim\,{}^t\Gamma])={}^t(\Gamma[pr_2\Gamma])$, откуда $\Gamma[pr_2\Gamma]\models W_1 = W_2$. Теорема доказана.

Следствие. Пусть выполняются условия теоремы 3. Тогда, если $y\notin C(W_1W_2)$, $y\neq x$, $\Gamma\models xW_1y=xW_2y$, то $\Gamma[(\ker\Gamma + pr_2\Gamma)/\ker\Gamma]\models W_1=W_2$.

Список литературы

1. Наумик, М.И. Полугруппа линейных отношений / М.И. Наумик // Доклады НАН Беларуси. – 2004. Т. 48, № 3. – С. 34–37.
2. Бирюков, А.П. Многообразия идемпотентных полугрупп / А.П. Бирюков // Алгебра и логика. – 1970. – Т. 9, № 3,. – С. 255–273.
3. Коряков, И.О. Линейные полугруппы идемпотентов / И.О. Коряков // Исследования по современной алгебре. – 1978. – Т. 11, № 3. – С. 54–96.

НЕКОТОРЫЕ АСПЕКТЫ ЗАЩИТЫ КОНТЕНТА В ИНФОРМАЦИОННЫХ СИСТЕМАХ АРХИТЕКТУРЫ КЛИЕНТ-СЕРВЕР

В.В. Новый

Витебск, УО «ВГУ им. П.М. Машерова»

В настоящее время большинство информационных систем строится на основе клиент-серверной или распределенной архитектуры. При этом для некоторых видов информационных систем особую роль играет защита контента от несанкционированного доступа или модификации информации. Одним из типов подобных систем являются приложения для проведения автоматизированного тестиро-