Półgrupa – prawie jak grupa?

Arkadiusz Męcel

Seminarium magisterskie: Klasyczne struktury algebraiczne
15 października 2009r.

Celem tego referatu jest zarysowanie podstaw teorii półgrup. Sama nazwa 'półgrupy' sugerować by mogła, że będzie to jakaś zubożona teoria grup, gdzie pewne charakterystyczne dla teorii grup fakty formułować będziemy musieli być może ogólniej, lub z większą ostrożnością. Nie jest to zupełnie bezzasadne podejrzenie. Tak się dzieje w wielu miejscach algebry, na przykład w teorii pierścieni, gdy ze znajomego gruntu przemiennego przenosimy się w nieprzemienne obszary; czy w teorii algebr skończenie wymiarowych, gdy porzucamy założenie o zerowaniu się radykału Jacobsona. W przypadku teorii półgrup sprawa ma się jednak zupełnie inaczej. Jak pokażemy dalej, opuszczenie założenia o odwracalności każdego elementu i posiadaniu jedynku dramatycznie zmienia własności rozważanej struktury algebraicznej.

Przejdźmy zatem do definicji:

Definicja 1 (Półgrupa) *Parę $(S, \circ)$, gdzie S – zbiór, $\circ : S \times S \to S$ – działanie dwuargumentowe, nazywamy półgrupą jeśli $\circ$ jest działaniem łącznym.*

W odróżnieniu do pojęcia grupy brakuje tu dwóch aksjomatów. Po pierwsze, w przypadku grup istnieje element e taki, że dla każdego $s \in S$ $e \circ s = s \circ e = s$. Gdy półgrupa posiada taki element nazywamy ją monoidem. Do grup brakuje więc tylko odwracalności każdego z elementów. Jest to, jak się okazuje poważne wymaganie.

1 Przykłady półgrup

Choć w zasadniczych kursach algebry nie ma miejsca na półgrupy, z podstawowymi przedstawicielami tych struktur zdążyliśmy się już kilka razy zetknąć. Spójrzmy na garść przykładów:

1. Rozpatrując dowolny pierścień łączny R, jeśli spojrzymy na niego jedynie pod kątem mnożenia, wówczas dostaniemy półgrupę. Może się to wydawać mało odkrywcze, ale w prowadzi do wielu namacalnych przykładów, a także do wielu trudnych zagadnień:

   (a) Po pierwsze, można rozważać liczby całkowite $\mathbb{Z}$ z mnożeniem. Charakterystyczne jest to, że wliczamy również 0. W strukturze tej siedzi wiele podpółgrup: liczby naturalne z mnożeniem, liczby złożone, wielokrotności danej liczby, potęgi liczb pierwszych... Z półgrupą Z^* wiąże się ciekawy problem otwarty. Podobnie jak w przypadku grup czy pierścieni, można mówić, że półgrupa jest generowana przez pewien zbiór X (pojęcie generowania należy do algebry uniwersalnej). Półgrupa $\mathbb{Z}^*$ nie jest skończenie generowana. Wiadomo to od mniej więcej 2500 lat :) Powstaje pytanie: czy jeśli wezmę półgrupę multiplikatywną R^* dowolnego nieskończonego pierścienia R, to będzie ona nieskończenie generowana? Wyniki w tej materii są bardzo świeże. Po pierwsze, nie wiadomo tego w pełnej ogólności. Co wiemy? Kilkanaście lat temu dowiedziono to na przykład dla wszystkich pierścieni przemiennych R. W 2000 roku ukazał się ogólniejszy dowód ([1]), obejmujący tzw. PI - pierścienie.[1] Nie wdając się w szczegóły, PI to skrót od polynomial identity, a więc mowa o takim pierścieniu, w którym nieprecyzyjnie mówiąc prawdziwa jest pewna równość wielomianowa (nawet przeliczalnie wielu zmiennych). Pierścień przemienny jest PI, bo spełnia równość $xy - yx = 0$.

(b) Rozważając pierścień macierzy rozmiaru $n \times n$ nad ciałem (lub pierścieniem) K dostajemy inny klasyczny przykład półgrupy. Są to macierze z mnożeniem. Mnożenie jest oczywiście łączne, jest jedynka, ale dobrze wiadomo, że nie każda macierz jest odwracalna.

2. Innym przykładem półgrupy jest półgrupa wolna na zbiorze X. Z punktu widzenia algebry uniwersalnej półgrupy tworzą rozmaitość, a więc klasę zamkniętą na podalgebry, obrazy homomorficzne i produkty. Może się to wydawać bardzo naturalne, ale na przykład ciała nie mają tej własności (produkt leży). Jeśli $X = \{a, b\}$, to półgrupa wolna generowana przez ten zbiór składa się ze wszystkich słów złożonych z nieprzemiennych liter a, b. Swoją drogą warto samemu zastanowić się czym taka półgrupa różni się od grupy wolnej o dwóch elementach...

3. Każda półgrupa powstaje przez podzielenie półgrupy wolnej nad pewnym zbiorem przez zbiór pewnych równości. Rozważmy jeden taki przykład:

$$S = \langle a, b \,|\, ab = 1 \rangle.$$

Półgrupę tą nazywamy monoidem bicyklicznym. Nazwa się razem wyjaśni. Nie wzgłębiając się na razie w formalną strukturę tej konstrukcji, powiedzmy po prostu, że rozważana półgrupa składa się ze wszystkich skończonych napisów złożonych z liter a, b z mnożeniem będącym konkatenacją napisów. Dodatkowo zakładamy, że napis ab możemy zawsze zastąpić przez 1. Okazuje się, że każdy element tej półgrupy można przedstawić jednoznacznie w postaci $b^i a^j, i, j \geqslant 0$. Operacja składania ma następującą postać:

$$(b^i a^j)(b^k a^l) = b^{i-j+\max(j,k)} a^{l-k+\max(j,k)}.$$

Łatwo zatem widzieć, że grupa bicykliczna jest izomorficzna z $\mathbb{N} \times \mathbb{N}$ z następującym mnożeniem:

$$(i, j)(k, l) = (i - j + \max(j, k), l - k + \max(j, k)).$$

Zauważmy, że rozważana w tym przykładzie półgrupa ma jednostronną jedynkę. Można zauważyć, że zbiór, na którym ją tworzymy jest nieskończony. Czy da się skończony przykład półgrupy z jednostronną jedynką? Okazuje się, że nie. Więcej, półgrupy z taką własnością są nieprecyzyjnie mówiąc, duże. Jeżeli rozważamy algebrę (przestrzeń liniową i pierścień ze zgodnymi strukturami), wówczas jeśli jej półgrupa multiplitatywna ma jednostronną jedynkę, wówczas wymiar tej algebry musi być nieskończony. Przykładem jest algebra endomorfizmów ciągów nieskończonych.

4. Kanoniczny przykład półgrupy jest następujący: Rozważamy niepusty zbiór X. Zbiór funkcji z X do X oznaczamy przez T_X i wprowadzamy na nim strukturę półgrupy poprzez składanie. Jest jasne,

[1] Ogólny dowód opiera się na standardowej, wspominanej na seminarium, metodzie redukcji. Najpierw dowodzimy dla pierścieni pierwszych, potem dla półpierwszych, a potem ogólnie...

że jest to działanie łączne. Tak uzyskaną półgrupę nazywamy pełnym monoidem transformacji z X do X. Dla zbioru skończonego elementy T_X reprezentować można podobnie jak permutacje. Wtedy złożenie dwóch przykładowych transformacji ma postać:

$$\begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,5\,2\,1\,3 \end{pmatrix}\begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,1\,4\,4\,2 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,1\,4\,4 \end{pmatrix}, \quad \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,1\,4\,4\,2 \end{pmatrix}\begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,5\,2\,1\,3 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,1\,1\,5 \end{pmatrix}.$$

Jest jasne, że nie mamy tu do czynienia z grupą. Jeżeli transformacja nie reprezentuje bijekcji zbioru X w siebie, wówczas nie można jej odwrócić. Zauważmy, że dla zbioru skończonego X mocy n każdy element $f \in T_X$ można reprezentować w postaci macierzy $n \times n$. W każdej kolumnie takiej macierzy znajdować się będzie dokładnie jedna jedynka (poza tym zera). W kolumnie j jedynka będzie stała dokładnie na tym miejscu i, na który przechodzi j-ty element zbioru X przy transformacji f. Złożeniu przekształceń odpowiada mnożenie odpowiednich macierzy. Ile jest takich macierzy? Łatwo widzieć, że n^n.

Dlaczego przykład ten jest kanoniczny? Przypomnijmy sobie, że w przypadku grup mieliśmy do czynienia z analogiczną sytuacją. Kanonicznym przykładem grupy były grupy bijekcji S_X dowolnego zbioru X w siebie. Z kursu teorii grup pamiętamy twierdzenie Cayleya, które mówi, że każda grupa określona na zbiorze X może być zanurzona jako podgrupa w pełnej grupie bijekcji zbioru X w siebie. W przypadku grup skończonych oznacza to, że grupa rzędu n może być zanurzona w grupie permutacji jako podgrupa. Grupa permutacji zbioru n elementowego jest natomiast reprezentowana w postaci macierzy $n \times n$, które w każdej kolumnie i w każdym wierszu mająą dokładnie jedną jedynkę. W teorii półgrup analogiczne twierdzenie jest prawdziwe. Każdą półgrupę określoną na zbiorze X traktować jako podpółgrupę pełnej półgrupy transformacji zbioru X. W przypadku półgrup skończonych oznacza to włożenie w odpowiednią półgrupę macierzy.

Swoją drogą, nie jest wcale trywialnym zagadnieniem stwierdzenie jaki jest najmniejszy rozmiar macierzy, w jakie włożyć można grupę permutacji zbioru n elementowego.

5. Na koniec tej części przedstawimy bardziej zaawansowany i bardzo istotny historycznie przykład. Jest on jednak również bardzo charakterystyczny. Nierzadko zdarza się, że badając jakąś sytuację widzimy, że przykładając do niej relację równoważności dostajemy zbiór klas, na którym można wprowadzić strukturę półgrupy (lub nawet chętniej) – grupy. Tak się dzieje na przykład w topologii, gdy rozważamy grupę podstawową czy wyższe grupy homotopii. W algebrze takich przykładów jest mnóstwo. Zobaczmy jeden z prostszych. Niech R będzie dowolnym niezerowym pierścieniem przemiennym, zaś $I(R)$ – zbiorem ideałów R. Wiadomo, że ideały I, J można mnożyć. Ale wynikiem nie jest zbiór elementów postaci $IJ = \{ij, i \in I, j \in J\}$, tylko ideał generowany przez ten zbiór. Można jednak zadać interesujące pytanie: kiedy IJ jest iloczynem ideałów I, J? Jest tak na pewno w pierścieniach ideałów głównych. Istotnie, iloczyn $(a)R \cdot (b)R = (ab)R$. A gdy własność ta nie jest spełniona? Wówczas wprowadzamy następującą relację równoważności:

   Powiemy, że niezerowe $I, J \in I(R)$ są równoważne (ozn. $I \sim J$) jeśli istnieją takie niezerowe ideały główne $A, B \in I(R)$, że $IA = JB$. Jest to relacja równoważności (sprawdzimy na zajęciach, potrzebna przemienność). Zbiór klas tej równoważności tworzy monoid ze względu na mnożenie klas indukowane z mnożenia ideałów z obustronną jedynką utworzoną przez klasę ideałów głównych. Wielkość tego monoidu jest miernikiem tego, jak bardzo iloczyny IJ różnić się mogą od ideałów. Przykład ten ma ważne zastosowanie w teorii liczb. Można bowiem zapytać jak sprawić, by półgrupa klas ideałów była grupą? Okazuje się, że potrzeba do tego dość specyficznej klasy pierścieni, zwanych pierścieniami Dedekinda. Jest to bardzo naturalna klasa pierścieni. Zachodzi w nich twierdzenie o jednoznaczności rozkładu na czynniki pierwsze. Nie elementów jednak (do tego trzeba być PID), ale ideałów. Skąd to się wzięło i jak to zobaczyć? Zaczęło się od wielkiego twierdzenia Fermata. W XVII wieku postawiono hipotezę na temat równania:

$$x^n + y^n = z^n.$$

Mówiła ona, że dla $n > 2$ nie ma ono rozwiązań w liczbach całkowitych x, y, z. Przez wieku próbowano różnych metod. Odkryto przy tym zaskakujące właści wielu obiektów, które dziś nazywamy pierścieniami. Jedna z nich wiąże się z półgrupą klas ideałów. Równanie powyższe można rozważać jedynie dla wykładników pierwszych p. Wtedy można rozważać następujący rozkład przy pomocy pierwiastka pierwotnego stopnia p z 1, nazwijmy go ζ_p:

$$x^p + y^p = (x+y)(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{p-1}y\right) = z^p$$

Okazuje się, że dla względnie pierwszych x, y czynniki po lewej są elementami pierwszymi pierścienia $\mathbb{Z}[\zeta_p]$. Mamy więc rozkład na czynniki nierozkładalne. Można by stąd wnioskować, że skoro po prawej stronie leży p - ta potęga, to każdy z czynników pierwszych musi być p-tą potęgą. Gdyby tak było, dalej rozwiązanie byłoby już nietrudne. Niestety, w rozumowaniu był błąd. Nie dla każdego p pierścień $\mathbb{Z}[\zeta_p]$ ma jednoznaczność rozkładu. Wiadomo, jak objawia się niejednoznaczność rozkładu. Biorąc na przykład pierścień $\mathbb{Z}[\sqrt{-5}]$ mamy:

$$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Wszystkie czynniki w tym rozkładzie są nierozkładalne, ale nie wszystkie są pierwsze. Stąd niejednoznaczność. Pechowo dla pomysłodawców, najmniejsze p, gdzie występuje załamanie dla $\mathbb{Z}[p]$ wynosi 23. Co więcej, w XX. wieku dowiedziono, że tylko dla 29 liczb pierwszych pierścień $\mathbb{Z}[\zeta_p]$ ma jednoznaczność rozkładu. Pachnie to pewną ironią. Jaki to ma związek z ideałami? Otóż, mozna rozważać ideały generowane przez elementy, gdzie rozkład jest niejednoznaczny. Na przykład w $\mathbb{Z}[\sqrt{-5}]$ mamy równość ideałów:

$$(2) \cdot (3) = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Co więcej, można napisać:

$$(2) \cdot (3) = (1+\sqrt{-5})(1-\sqrt{-5}) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

Ideały na końcu tej równości są ideałami pierwszymi. Okazuje się, że rozkład ten jest jednoznaczny. Pierścień $\mathbb{Z}[\sqrt{-5}]$ nie ma jednoznaczności rozkładu. Ale jest pierścieniem, który ma grupę klas ideałów. Grupa ta jest dwueelementowa. W połowie XIX wieku wykazano, że także w każdym pierścieniu $\mathbb{Z}[\zeta_p]$ zachodzi twierdzenie o jednoznacznym rozkładzie na ideały pierwsze. Okazało się, że równość:

$$(x+y)(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{p-1}y\right) = (z)^p$$

jest równością rozkładów na ideały pierwsze. Stąd powstało sporo częściowych rozwiązań WTF. Z półgrupą i grupą klas ideałów wiąże się mnóstwo interesujących zagadnień (cała dziedzina algebraicznej teorii liczb), a także wiele nierozwiązanych problemów.

2 Grupy a półgrupy

Na półgrupę można patrzeć dwojako: z jednej strony jako na niezwykle ubogą i ogólną strukturę algebraiczną; z drugiej zaś: jako na naturalne uogólnienie dobrze znanego (i historycznie rzecz biorąc wcześniej uznanego za istotne dla matematyki) pojęcia grupy. Jak pokażemy, choć obydwie te intuicje pojęcia półgrupy mają naturalne potwierdzenie we własnościach tej struktury, nie są one bynajmniej ze sobą zgodne.

W dalszej części referatu postaramy się ukazać fundamentalne różnice strukturalne pomiędzy półgrupami i grupami. W tej chwili wskażemy jedynie kilka faktów motywujących takie postępowanie. Zacznijmy od wyników ilościowych. Na kursie teorii grup niemało uwagi poświęcamy ilości izomorficznych typów grup danego rzędu. Stosunkowo nietrudno sklasyfikować wszystkie grupy rzędu mniejszego od 10. Jak jest z półgrupami? Mamy oczywiście znacznie więcej swobody. Wydaje się, że jest to zadanie kombinatoryczne, półgrupy kojarzą się nam z funkcjami z jednego zbioru do drugiego i skoro odrzucamy niewygodne założenie odwracalności, to liczenie powinno być łatwiejsze. Okazuje się, że tak nie jest. Łączność, która odróżnia półgrupy od grupoidów, to niezwykle sztywne założenie. Spójrzmy na następującą tabelkę:

n	Liczba grup	Liczba półgrup
1	1	1
2	1	4
3	1	18
4	2	126
5	1	1160
6	2	15973
7	1	836021
8	5	1843120128
9	2	??? > 50000000000000

Można z niej odczytać ile jest, z dokładnością do izomorfizmu, grup rzędów n, $1 \leqslant n \leqslant 9$ oraz ile jest, z dokładnością nie tylko do izomorfizmu, ale też do antyizomorfizmu, półgrup rzędu n. Do dziś nie wiemy ile jest półgrup rzędu 9... Wyniki dotyczące ilości półgrup rzędu 7 i 8 pochodzą z lat 90. XX wieku. To zestawienie pozwala przypuszczać, że uzyskiwanie jakichkolwiek ogólnych twierdzeń podobnych do klasyfikacji skończonych grup prostych, może być w przypadku półgrup niemożliwe.

3 Kilka słów o strukturze półgrup skończonych...

Naturalne różnice pomiędzy półgrupami i grupami wynikają z możliwości istnienia w półgrupach takich elementów jak: zera, jednostronne zera, jednostronne jedynki. O wszystkich tych sytuacjach wspomnieliśmy już wcześniej. Są to jednak różnice pobieżne. Półgrupy różnią się od innych struktur algebraicznych w sposób mający swe korzenie w algebrze uniwersalnej. Rzecz leży w możliwościach dzielenia półgrup przez... no właśnie, przez co? Powiedzmy przez co dzielimy w półgrupach:

Definicja 2 (Ideał) *Podzbiór $I \subset S$ nazywamy ideałem lewostronnym w półgrupie S jeśli $SI = \{si, s \in S, i \in I\}$. Analogicznie definiujemy ideał prawostronny i obustronny półgrupy S.*

Pomysł na ten warunek nie wydaje się zapewne dziwny. Dziedziczymy pomysł z teorii pierścieni. I tak jak każdy pierścień można pozbawić struktury addywnej, tak i każdy jego ideał można. W otrzymanej półgrupie dostajemy więc w naturalny sposób ideały półgrupowe. Niespodzianka polega na tym, że nie dostaniemy jeszcze wszystkich ideałów półgrupowych. Fakt ten może się wydawać intuicyjnie jasny, ma on jednak głębokie podłoże.

Jeśli przypomnimy sobie teorię pierścieni, to pamiętamy, że każdemu ideałowi I pierścienia R odpowiada dokładnie jeden homomorfizm R w R. Jak to się dzieje? Weźmy dla przykładu $R = \mathbb{Z}$. Jest to pierścień ideałów głównych i każdy ideał ma postać $n\mathbb{Z}$, $n \in \mathbb{N}$. Rozważmy teraz dowolny homomorfizm $h : \mathbb{Z} \to \mathbb{Z}$. Załóżmy, że ma on niezerowe jądro. Wówczas musi ono być ideałem. Istotnie, jeśli $h(a) = 0$, to $h(ab) = 0$ oraz $h(ba) = 0$ dla każdego $b \in \mathbb{Z}$. Jest to ideał główny, a więc zbiór postaci $n\mathbb{Z}$. I odwrotnie, jeśli mamy ideał $I = n\mathbb{Z} \lhd \mathbb{Z}$, to odpowiada mu homomorfizm $h(z) = t$, gdzie t to reszta z dzielenia z przez n. Łatwo widzieć, że mamy tu wzajemnie jednoznaczną odpowiedniość pomiędzy ideałami a jądrami homomorfizmów. O jądrach tych można myśleć jeszcze inaczej. Jeśli spojrzymy na nasz homomorfizm, to można rozważyć relację $a \equiv_h b \Leftrightarrow h(a) = h(b)$. Dla liczb całkowitych jest to po prostu jedna z relacji przystawania modulo n. Jądro homomorfizmu to nic innego tylko klasa zera przy tej relacji. Innymi słowy, można wskazać odpowiedniość pomiędzy ideałami $\mathbb{Z}$, a relacjami przystawania modulo n. Ukrywa się w tym bardzo ogólna myśl. Jak wiadomo, przystawanie modulo n jest odporne na branie elementu przeciwnego, dodawanie stronami oraz mnożenie stronami – a więc na wszystkie operacje pierścieniowe. Relacje, które mają podobną odporność można wprowadzać w dowolnym pierścieniu i nazywamy je kongruencjami. Okazuje się, ze ideały pierścienia R są we wzajemnie jednoznacznej odpowiedniości z kongruencjami na R. Podobnie rzecz się ma z grupami i podgrupami normalnymi.

Spójrzmy jednak teraz na $\mathbb{Z}^*$, a więc pierścień pozbawiony struktury addytywnej. Przenieśmy też bezpośrednio ideały, odrzucając strukturę grupy abelowej. Są to dalej zbiory wielokrotności odpowiednich liczb. Oczywiście dalej każdemu z nich odpowiada homomorfizm półgrup polegający na przydzielaniu reszty z dzielenia przez n. Ale w półgrupie $\mathbb{Z}^*$ jest znacznie więcej ideałów! Weźmy na przykład zbiór liczb różnych co do wartości bezwzględnej od 1. Niewątpliwie jest to ideał półgrupowy, bo cokolwiek przemnożymy przez liczbę różną od 1, jedynki nie dostaniemy. Ale nie istnieje homomorfizm półgrupowy, którego ideał ten byłby jądrem. Relacja $a\mathcal{R}b \Leftrightarrow |a - b| \neq 1$ nie jest kongruencją, nie jest to nawet relacja równoważności (nie zgadza się przechodniość: np. $a = 5, b = 2, c = 4$). Z ogólnego punktu widzenia jest jasne, że ideały półgrupowe to coś innego niż jądra kongruencji. Zauważmy, że w przypadku grup, ideały półgrupowe to całe grupy, a mimo to dzielniki normalne mogą istnieć. Po co nam więcej ideałów niż algebra uniwersalna zakłada? Mamy trudniejszą strukturę do objęcia, okazuje się, że ideały półgrupowe dają dobre efekty przy formułowaniu twierdzeń strukturalnych.

W półgrupach oczywiście ideały są po to, aby określać iloraz. Nie jest to czysta ogólno algebraiczna procedura, a twór zupełnie inny. Nazywamy go ilorazem Reesa R/I. Nie jest to zbiór klas równoważności, tylko: $R \setminus I \cup \{\theta\}$ ze strukturą mnożenia:

$$ab = \begin{cases} ab, & ab \notin I \\ \theta, & ab \in I \end{cases}.$$

Do twierdzeń klasyfikacyjnych wykorzystuje się zwykle struktury „proste”. W półgrupach będą to takie, które nie będą miały nietrywialnych ideałów. Nowością jest fakt, że w półgrupach, a więc obiektach z zasady przypominających strukturę multiplikatywną pierścienia, są też zera. Zera utrudniają patrzenie na ideały, bo ideał zerowy jest z zasady nietrywialny... Mimo to jest mało ciekawy. Dlatego jeśli półgrupa ma zero, to nazywamy ją 0-prostą jeśli nie ma nietrywialnych ideałów, oraz S^2 nie ma zerowego mnożenia. Oznacza to dokładnie tyle, że nie tylko nie zawiera żadnego ideału, ale nie jest też (sama jako ideał w czymś większym) tym feralnym zerowym przypadkiem.

Jak wyglądają twierdzenia strukturalne dla półgrup? Podamy tutaj interpretację w przypadku półgrup skończonych. Sposób, w jaki tworzymy grupę ilorazową, a więc de facto zastępowanie ideału zerem nasuwa pewien plan. Bierzmy półgrupę skończoną S. Ona ma jakieś ideały, ale też skończenie wiele. One jakoś się w sobie zawierają, tworzą więc jakiś porządek częściowy. Skoro jest to porządek skończony, to w istocie jest to suma skończenie wiele łańcuchów. Weźmy element maksymalny z każdego z nich. Cała półgrupa jest zatem sumą tych elementów maksymalnych. A więc półgrupę już umiemy jakoś poszatkować. Można jednak dokładniej. Jak spojrzymy na każdy z łańcuchów, gdzie maksymalny niezerowy element to I to jest tam minimalny niezerowy element J_1, a po nim jest J_2 itd. Wytnijmy J_1 ilorazem Reesa. Teraz w tym co zostało, a więc w $I \setminus J_1 \cup \theta$ jest znowu jakiś porzadek na ideałach. Okazuje się, że jest to łańcuch, dokładnie dziedziczony z wyjściowego. A więc minimalny w nim jest J_2/J_1. I tak można ładnie pociąć każdy łańcuch na plasterki. Każdy z nich natomiast jest, i to się dowodzi łatwo, albo półgrupą 0-prostą, albo półgrupą z zerowym mnożeniem. Półgrupy 0-proste są tymczasem dobrze opisane.

Definicja 3 (Półgrupa macierzowa Reesa) *Dana jest grupa G, dwa niepuste zbiory X, Y (można o nich myśleć jak o zbiorach skończonych, choć nie jest to konieczne), oraz macierz P o wymiarach $Y \times X$ o elementach z G. Jest to więc funkcja $Y \times X \to G$ dana wzorem $(y, x) \to p_{yx}$. Rozważam teraz zbiór $G \times X \times Y$ i wprowadzam na nim następujące mnożenie:*

$$(g, x, y) \circ (g', x', y') = (gp_{yx'}g', x, y').$$

Jest to półgrupa i oznaczamy ją jako $\mathcal{M}(G, X, Y, P)$.

Jak rozumieć tak utworzoną strukturę? Wyobraźmy sobie, że element $(g, x, y) \in S$ jest macierzą o wymiarach $X \times Y$, której jedynym niezerowym miejscem jest miejsce w kolumnie y i rzędzie x i na tym miejscu stoi element g. Co oznacza mnożenie w naszej półgrupie? Jeśli weźmiemy dwie macierze A, B odpowiadające pewnym $(g, x, y), (g', x', y')$, to mamy:

$$A \circ B = APB.$$

Okazuje się, że każda półgrupa skończona 0-prosta jest jedną z wyżej wymienionych. Może to się wydawać bardzo dziwne, zważywszy na to, że możemy przecież konstruować bardzo egzotyczne półgrupy skończone. Dla nich jednak zwykle zbiory X, Y są bardzo niewielkie, a grupa G nieskomplikowana.
Niedobór kongruencji w stosunku do ideałów wymusza rozważanie dodatkowej klasy relacji, które pozwolą na skuteczny opis struktury półgrupy. Wyróżnia się w tym celu tzw. relacje Greena. Dwa elementy $a, b \in S$ są w takiej relacji (odpowiednio $a\mathcal{L}b, a\mathcal{R}b, a\mathcal{J}b$) jeśli równe są ideały generowane przez nie (lewostronne $S^1a = S^1b$, prawostronne $aS^1 = bS^1$, obustronne $S^1aS^1 = S^1bS^1$). W przypadku macierzy odpowiednie relacje oznaczają na przykład: izomorfizm jąder macierzy, izomorfizm obrazów macierzy, równość rzędów macierzy. Klasy relacji Greena grają kluczową rolę w dowodzie tw. Reesa o postaci półgrup 0-prostych.

W referacie omówiony został dokładniej przykład $M_n(\mathbb{K})$. Choć jest to półgrupa nieskończona, posiada ona jedynie jeden skończony łańcuch ideałów. Nie jest to bardzo dziwne. Macierze jako pieeścień są proste, a więc półgrupowych ideałów za dużo mieć nie mogą. Każdy z 0-prostych faktorów to nic innego tylko macierze rzędu j z dołączonym zerem. Szczegóły czytelnik odnajdzie w [4].

Literatura

[1] BELL K., KLEIN A.: *On the multiplicative semigroup of a ring*, Israel Journal of Mathematics 116 (2005), str. 249-252.

[1] HOWIE J.M.: *An introduction to semigroup theory*, Londyn (1976).

[2] GRILLET P.A: *Semigroups. An introduction to the structure theory*, CRC Press (1995).

[3] MITCHELL J.D.: *Semigroup theory. Course notes*, Univ. Saint Andrews, Szkocja (2008).

[4] OKNIŃSKI J.: *Semigroups of matrices*, World Scientific 1998.

[4] MURGEL P.V.: *On group and semigroup algebras*, praca doktorska dostępna online: www.impa.br/opencms/pt/ensino/downloads/teses_de_doutorado/teses_2006/paula_murgel.pdf (2006).