Nieprzemienne pułapki

Arkadiusz Męcel

Koło Pasjonatów Matematyki

14 maja 2009r.

Streszczenie

W nieprzemiennym świecie spełniają się najgorsze matematyczne sny... Funkcje kwadratowe mają nieskończenie wiele pierwiastków. Nie ma ułamków, a jeśli nawet są, to są te prawicowe, a lewicowe dawno wyginęły! Macierze o niezerowych wyznacznikach nie chcą się odwracać... A właściwie to wyznaczniki są bez sensu! O tych i innych jakże przerażających możliwościach opowiem na najbliższym posiedzeniu Koła Pasjonatów Matematyki!

Zanim zagłębimy się w koszmarny sen o nieprzemienności zacznijmy od innej, z pozoru, bajki. Na pierwszym roku studiów słuchamy wykładu z GALu. A tam zdarza pojawia się niekiedy następującej treści twierdzenie:

Twierdzenie 1 (Cayley – Hamilton) *Każda macierz zespolona spełnia swój wielomian charakterystyczny.*

Aby unaocznić ten fakt możliwie niewielkim kosztem sprawdźmy pierwszy z brzegu, prosty przykład:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

Wielomian charakterystyczny to:

$$(1-\gamma)(4-\gamma)-6=\gamma^2-5\gamma-2.$$

Tymczasem:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^2 - 5\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} - 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix} - \begin{pmatrix} 5 & 10 \\ 15 & 20 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Twierdzenie to ma rozmaite dowody. Pierwsze z nich pochodzą jeszcze z XIX wieku – choć jak to często w matematyce bywa – nie od domniemanych autorów. Cayley w istocie sformułował to twierdzenie w 1858 roku, ale za zasadne uznał dowodzić go jedynie w wersji dla macierzy wymiaru 2×2 oraz 3×3.[1] Może więc Hamilton? Ojciec kwaternionów nie wniósł nic poza dowodem w przypadku 4×4. Tym, który po raz pierwszy dowiódł to twierdzenie w pełnej ogólności był Ferdinand Georg Frobenius. Stało się to w 1896 roku. Profesor Uniwersytetu w Berlinie był na tyle hojny by to w Arthurze Cayleyu widzieć twórcę tego faktu. Jako tradycjonalista wyrażał zapewne stare już wówczas przekonanie, że twierdzenie należy nazywać imieniem pomysłodawcy, a nie tego, który dowodzi. Na marginesie warto więc chyba dodać, że to właśnie Frobenius podał pierwsze ogólne dowody tak fundamentalnych faktów jak: twierdzenie Sylowa, klasyfikacja skończenie generowanych grup abelowych, lemat Burnside'a o zliczaniu orbit. Tyle tytułem dygresji.

[1] Cayley, Memoir on the theory of matrices (1858)

Czas na fałszywy dowód wspomnianego twierdzenia. Jak nierzadko w matematyce – to fałszywe dowody, w przeciwieństwie do prawdziwych, stymulują ciekawe dyskusje.

'Dowód' nasz ma jedną linijkę. Niech $w_A(x)$ – wielomian charakterystyczny macierzy A. Jest to jak wiadomo $\det(A - xI)$. Wstawmy więc zamiast x macierz A i dostaniemy:

$$w_A(A) = \det(A - AI) = \det(A - A) = \det(0) = 0.$$

Gdzie leży oszustwo? Oczywiście w pierwszej równości. $w_A(A)$ jest macierzą, tymczasem $\det(A - AI)$ jest skalarem. Wydaje się, że nie jest to poważny problem. Można to przecież jakoś ratować, na przykład przemnożyć $\det(A - AI)$ przez macierz I i wtedy już wszystkie wyrażenia są macierzami:

$$w_A(A) = \det(A - AI)I = \det(A - A)I = \det(0)I = 0.$$

Wciąż źle? Czyżby równość $w_A(B) = \det(A - BI)I$ była nieprawdziwa dla macierzy kwadratowych $A, B \in M_n(\mathbb{R})$? Weźmy macierze:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Wielomian charakterystyczny macierzy A wynosi $w_A(x) = x^2 - x$. Tymczasem jeśli podstawimy do tej równości macierz B dostaniemy $w_A(B) = B^2 - B = 0 - B = -B$. $\det(A - BI)I$, a wiec domniemana wartość $w_A(B)$ wynosi natomiast $\det(A - B)I = 0$. Widać, że zaprezentowane podejście nie jest dobre...

* * *

Czy to wszystko ma cokolwiek wspólnego z nieprzemiennością? Okazuje się, że tak! To, co jest nieprzemienne w naszym dotychchczasowym przykładzie to macierze. Jak wiadomo, na zbiorze macierzy kwadratowych wymiaru n można wprowadzić strukturę pierścienia łącznego z jedynką. Nie jest to jednak pierścień przemienny. Nietrudno się o tym przekonać patrząc na iloczyny AB, BA macierzy zaprezentowanych wyżej. Dobrze wiec – macierze są nieprzemienne, ale o tym wiedzieliśmy już wcześniej. Dlaczego rozumowanie wyżej zawiera usterkę, której nie dostrzegamy? Są jeszcze owe wielomiany charakterystyczne, w które bardzo chcieliśmy podstawiać macierze. Tu właśnie, jak się okazuje, polegliśmy z kreteresem.

Przypomnijmy sobie: co to jest wielomian? Otóż, jest to formalny napis postaci:

$$w = r_0 + r_1 x + r_2 x^2 + \ldots + r_n x^n, \quad r_i \in R$$

Możemy wykonywać formalne operacje mnożenia i dodawania takich napisów. Dodajemy 'zwyczajnie' po współrzędnych, mnożymy zaś wedle reguły:

$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) X^k.$$

O czym my natomiast myślimy? Zwykle o funkcji wielomianowej $w(x)$, która dla jakiegoś $a \in R$[2] przyjmuje wartość:

$$w(a) = r_0 + r_1 a + r_2 a^2 + \ldots + r_n a^n \in R$$

Wydaje się więc, że znamy tę bajkę – 'funkcja wielomianowa, to nie to samo, co wielomian', bo na przykład w pierścieniu reszt z dzielenia przez 4 wielomiany $f_1 = x^4 + 1$ oraz $f_2 = 1$ mają tożsame funkcje wielomianowe. Wiadomo więc o co chodzi, prawda? Otóż jest gorzej, niż się zdaje!

[2] Choć można ogólniej...

Czym jest dokładnie funkcja wielomianowa? Funkcja wielomianowa to przyporządkowanie działające w następujący sposób:

$$a \to v_a[w],$$

gdzie $v_a(w)$ przyporządkowuje wielomianowi w 'wartość w a', a więc element:

$$r_0 + r_1 a + r_2 a^2 + \ldots + r_n a^n \in R.$$

Przyzwyczailiśmy się do pewnych własności ewaluacji, bo tak nazywamy funkcję v. Na przykład do tego, że jest to homomorfizm pierścieni:

$$v_a(w + w') = v_a(w) + v_a(w'), \quad v_a(w \cdot w') = v_a(w) \cdot v_a(w').$$

Zwykle nie myślimy o tym w taki algebraiczny sposób – w końcu podstawienie, to podstawienie – jakąś wartość zawsze da! W przypadku nieprzemiennym, spotka nas niespodzianka!

Weźmy nasze dwie macierze A, B i rozważmy wielomiany (zdefiniowane jak wyżej), o współczynnikach w pierścieniu $M_2(\mathbb{R})$ postaci:

$$f = x, \quad g = B.$$

Teraz będziemy wykonywać 'podstawienia':

$$f(A) = A, \quad g(A) = B, \quad fg = Bx, \quad (fg)(A) = BA, \quad f(A)g(A) = AB.$$

I wyszło, że $(fg)(A) \neq f(A)g(A)$. Widać skąd pochodzi źródło problemu. W rozważanym przypadku logiczniejszym wydaje się, by iloczyn wielomianów f i g był zapisany w postaci xB. Ale przecież nie zapisujemy tak wielomianów. Zauważmy, że z definicji 'zwykłego mnożenia wielomianów' wynika między innymi fakt, że napisy formalne rx oraz xr, gdzie r – współczynnik, są równoważne (aby to mnożenie miało sens). Musimy wiedzieć co zrobić, gdy przy mnożeniu pojawi się coś pokroju xr. Zwykle zamieniamy po prostu kolejność. Tak jednak wolno nam robić tylko w przypadku wielomianów o współczynnikach przemiennych. Inaczej wszystko określimy poprawnie, ale niewiele z tym zrobimy.

Nikt jednak nie mówi, że napis xr musi się koniecznie zamienić w rx. Może jakby się zamieniał w coś innego, to problem przestałby istnieć? Niekoniecznie, ale mimo to obiekty takie istnieją. W przypadku wielomianów definiowanych dla pierścieni o nieprzemiennych współczynnikach, rozważa się często tzw. wielomiany skośne $R[x, \sigma, \delta]$, gdzie $\sigma : R \to R, \delta : R \to R$ są endomorfizmami takimi, że:

$$xr = \sigma(r)x + \delta(r).$$

W zależności od tego jak określimy σ, δ dostaniemy różne, dobrze zdefiniowane pierścienie wielomianów, w których będzie miało sens np. mnożenie wielomianów. Czy to uwolni nas od problemów z ewaluacją? Otóż nie! Może się okazać, że 'tradycyjnie' określona ewaluacja dalej nie będzie homomorfizmem. Nawet, gdy nim będzie, mogą się pojawić nieoczekiwane problemy.

Wszyscy pamiętamy czym jest pierścień kwaternionów. To takie większe liczby zespolone, gdzie zamiast jednego tylko i mamy i, j, k, każde w kwadracie daje -1, poza tym $ij = k, jk = i, ki = j$. Spróbujmy stworzyć sobie konkurencyjne pierścienie wielomianów nad tymi kwaternionami. Jeden będzie tradycyjny: $\mathbb{H}[x]$, gdzie porządkujemy współczynniki przy pomocy przemiennych praw. Na drugim zaś określamy przechodzenie tak:

$$xi = -ix, \quad xj = -jx, \quad xk = -kx.$$

Mamy więc jednoznacznie określoną funkcję $* : \mathbb{H} \to \mathbb{H}$ taką, że: $\mathbb{H}[x, *]$ jest pierścieniem wielomianów skośnych. Wprowadźmy możliwość podstawiania kwaternionów i rozważmy iloczyn wielomianów postaci:

$$f_1 = x - i, \quad f_2 = x - j.$$

Mamy więc wielomian $h(x) = (x - i)(x - j)$. Jeśli rozłożymy go zgodnie z tradycyjnymi zasadami, dostaniemy:

$$x^2 - (i + j)x + ij.$$

Jeśli postąpimy dokładnie tak, jak nakazuje nasza skośna funkcja $*$, to mamy:

$$x^2 - ix - xj + ij = x^2 - ix + jx + ij.$$

Żadna różnica? Niezupełnie. Policzmy wartości tych dwóch możliwych wersji w i. W pierwszym przypadku wychodzi nam $2k$, w drugim 0. Spojrzawszy na postać wyjściową widać, że 'intuicji' bliższa jest 'skręcona wersja'. Intuicji, to znaczy twierdzeniu Bezout, w końcu wartość powinna być zerem, skoro mamy czynnik $(x - i)$, prawda? Tak naprawdę okazuje się, że w przypadku skośnym ewaluacja jest homomorfizmem pierścieni, a w przypadku normalnym – nie!

To wcale nie koniec problemów z podstawianiem. Wprawdzie w skośnej wersji mamy dobre własności podstawiania, ale czy wartości tego podstawiania spełniają nasze oczekiwania? Weźmy

$$f = x^2 + 1 \in \mathbb{H}[x, *].$$

Policzmy jego wartość w i. Wychodzi 0. A w j? Znowu 0. A w k? Jak wyżej. Trochę dużo miejsc zerowych jak na wielomian stopnia 2. Ale przecież twierdzenie Bezout działało dla ciał, a kwaterniony to nie ciało! To prawda, zauważmy jednak, że poza nieprzemiennością, nic kwaternionów od zwykłego ciała nie różni. W literaturze obiekty takie nazywamy pierścieniami z dzieleniem lub inaczej: ciałami nieprzemiennymi. W takich twierdzenie Bezout nie działa. I to nie działa bardzo. Nasz wielomian ma więcej niż trzy zera. Przecież, jeśli: $a = bi + cj + dk$, to $a^2 = -(b^2 + c^2 + d^2)$. Dobierając więc tak b, c, d, by: $b^2 + c^2 + d^2 = 1$ widzimy, że wielomian nasz ma nieskończenie wiele pierwiastków! Widać więc, że podstawiać wolno, ale pożytku z tego wiele nie będzie...

Na własne oczy zobaczyliśmy, że podstawowa operacja, jaką jest podstawianie wartości wielomianu kompletnie traci swe naturalne własności gdy rozważać ją w nieprzemiennym kontekście. To tylko jeden z przykładów – omówiliśmy go dość szczegółowo by zaprezentować delikatność leżącą w tym właśnie miejscu, gdzie przemienność jest dla podtrzymania naszej intuicji kluczowa. Oczywiście, nie tylko wielomiany sprawiają problemy...

* * *

Zapowiedzieliśmy we wstępie, że będą problemy z wyznacznikiem. Czy można rozważać wyznacznik nieprzemienny tak samo jak w przypadku przemiennym? Można. Czy to ma sens? Niewielki: Spójrzmy na macierze:

$$\begin{pmatrix} i & i \\ j & j \end{pmatrix}, \quad \begin{pmatrix} i & j \\ i & j \end{pmatrix}$$

Wyznacznik macierzy 2 na 2 wyraża się wzorem $a_{11}a_{22} - a_{12}a_{21}$. W przypadku pierwszej macierzy jest to jest to $ij - ij = 0$ – zgodnie z oczekiwaniem. W drugim – jest gorzej, bo uzyskaliśmy $2k$. Jeśli byśmy jednak przez przypadek pomylili kolejność czynników a_{12} oraz a_{21} dostalibyśmy odwrotną odpowiedź. Pierwszym, który w 1845 roku zwrócił uwagę na ten problem był wspominany już wcześniej Arthur Cayley. Zaproponował on też proste wyjście. Jeśli nie wiemy, które z wyrażeń jest 'lepsze' jako wyznacznik, wybierzmy po prostu jedno z nich. Widać już jednak, że żaden wybór nie będzie dla nas w pełni satysfakcjonujący. W zależności od tego jaką definicję przyjmiemy, jedna z rozważanych macierzy stanie się nieosobliwa. W związku z tym, że lubiliśmy używać macierzy do rozwiązywania układów równań, jesteśmy zaniepokojeni brakiem tej opcji. Istnieją smutne konsekwencje tego faktu. Załóżmy, że wyznacznik macierzy:

$$\begin{pmatrix} i & j \\ i & j \end{pmatrix}$$

równy jest 2k (klasyczna definicja). Czy macierz ta jest odwracalna? Otóż nie! Istotnie, jeśli istnieje macierz kwaternionowa postaci:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

taka, że:

$$\begin{pmatrix} i & j \\ i & j \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

to oznacza nic innego tylko:

$$\begin{cases} ia + jc = 1 \\ ib + jd = 0 \\ ia + jc = 0 \\ jb + jd = 1 \end{cases}$$

Kompletny absurd. Z drugiej strony podobnie. Jest więc bardzo źle. Macierz o niezerowym wyznaczniku nie ma odwrotności.

Idźmy jednak dalej. Spójrzmy na macierze:

$$A = \begin{pmatrix} i & 0 \\ 0 & j \end{pmatrix}, B = \begin{pmatrix} k & 0 \\ 0 & i \end{pmatrix}$$

Zauważmy, że:

$$\det(A)\det(B) = ijki = kki = -i, \quad \det(AB) = ikji = -jji = i.$$

Nie jest zatem spełnione twierdzenie Cauchy'ego. Kolejna z podstawowych własności wyznacznika upadła: nie jest to już homomorfizm, a to bardzo bardzo w nim ceniliśmy. Widać zatem czarne chmury na horyzoncie... Wrócimy do nich, uzbrojeni w wiedzę o nieco szerszej klasie pierścieni nieprzemiennych niż ta, którą dysponujemy obecnie.

* * *

Do tej pory mówiliśmy o znanych przykładach pierścieni nieprzemiennych. Jakby nie patrzyć, kwaterniony, czy macierze – to znane nam od dawna i mimo wszystko jakoś, mniej lub bardziej, akceptowalne przez nas obiekty. Potrzebujemy ich, więc niezależnie od komplikacji, musimy z nimi jakoś żyć. Takie pierścienie to dopiero przedpole prawdziwie mrocznych rejonów, istnych siedlisk Prawdziwie Nieprzemiennych Pierścieni. Granicą bezpiecznego terytorium jest skończony wymiar. Kwaterniony, intuicyjnie nawet to widać, mają jako przestrzeń liniowa, wymiar 4 nad liczbami rzeczywistymi. Macierze to, jak wiemy z GALu, przestrzenie liniowe wymiaru n^2 (o ile są nad ciałem), a więc też skończenie wymiarowy obiekt. Oczywiście, aby była mowa o nieprzemienności musi istnieć, zarówno w kwaternionach, jak i w macierzach, obok struktury przestrzeni liniowej, struktura pierścienia (a więc mnożenie). W ten sposób, o ile struktury te są zgodne, dostajemy tzw. algebry nad ciałem. Wersja nieprzemienności, która mówi, że czasem ab to nie to samo co ba, to wersja łagodna. Spójrzmy tymczasem na następujący przykład:

Rozważmy przestrzeń l_2, a więc takich ciągów, których szeregi kwadratów są zbieżne. Formalnie rzecz biorąc, dwa ciągi można do siebie dodać, można je przez siebie przemnożyć i można je mnożyć przez skalar. Mamy więc nieskończenie wymiarową przestrzeń liniową nad, $\mathbb{R}$ – powiedzmy. Jak jest przestrzeń liniowa, to są i endomorfizmy. Je też można dodawać i składać, a więc to pierścień przekształceń. Weźmy dwa z nich. Jedno, e_1, działa na ciągu $(x_n)_{n=0}^{\infty} \in l_2$ tak:

$$e_1(x_n) = x_{n+1}.$$

Drugie zaś, e_2, tak:

$$e_2(x_0) = 0, \quad e_2(x_n) = x_{n-1},\ n > 0.$$

e_1 i e_2 to po prostu przesunięcia – w prawo, i w lewo. No to spójrzmy na iloczyn: $e_1 \circ e_2 = Id$. Tymczasem $e_2 \circ e_1 \neq Id$. Widzimy, że e_2 jest elementem odwracalnym z lewej strony, ale to, co go z lewej strony odwraca, z prawej już nie chce! Co więcej, nietrudno uwierzyć, że w ogóle nie istnieje lewa odwrotność e_2 w pierścieniu endomorfizmów l_2. Istnienie jednostronnych odwrotności w pierścieniu, to już poważniejszy problem niż brak przemienności. Można na przykład udowodnić, że nie istnieje skończenie wymiarowa algebra nad ciałem, w której takie obiekty by istniały. Dlatego też większość osobliwych pierścieni nieprzemiennych istnieje jedynie w świecie nieskończonego wymiaru. Istnieje szereg algebraicznych powodów, dla których tak jest, ale to nie miejsce by o nich mówić.

Aby pokazać drobne zastosowanie naszej nowej wiedzy zobaczymy jak głęboce inna jest struktura znanych podgrup macierzy od tych znanych z przypadku przemiennego. Weźmy na przykład macierze górnotrójkątne. Wiemy, że nie wszystkie macierze się odwracają, więc ograniczmy się tylko i wyłącznie do takich, które mają porządne odwrotności z obydwu stron. Zwykle tworzyły one podgrupę macierzy. Teraz nie ku temu żadnego powodu:

$$\begin{pmatrix} e_1 & 1 \\ 0 & -e_2 \end{pmatrix}.$$

Macierz ta jest odwracalna, ale jej odwrotność ma postać:

$$\begin{pmatrix} e_1 & 1 \\ 1 - e_2e_1 & -e_2 \end{pmatrix}.$$

Nie jest to więc macierz górnotrójkątna. Oczywiście, definiuje się w przypadku nieprzemiennym analogi wszystkich podgrup klasycznych, ale trzeba zawsze zaznaczyć, że zarówno macierz, jak i jej odwrotność musi spełniać określoną regułę. Dość powiedzieć, że istnieją pierścienie, nad którymi odwrotności macierzy górnotrójkątnych są dolnotrójkątne.

* * *

Dużo już powiedzieliśmy, a tak naprawdę to dopiero wierzchołek góry lodowej. Istnieje wiele pojęć znanych ze świata przemiennego, ściślej związanych z algebrą, które wymagają delikatnych odpowiedników w nieprzemiennej wersji. Chociażby dziedziny, ideały pierwsze, pojęcia jednoznaczności rozkładu na czynniki czy też na przykład... ułamki. O nich więc na koniec. Wydaje się, że nic prostszego niż mieć ułamki. Tymczasem, łatwo się przekonać, że określając prawa działań na ułamkach znowu korzystamy z przemienności. Istnieją pierścienie, które w ogóle ułamków mieć nie mogą, choć nie mają ani jednego dzielnika zera. Istnieją takie, które mają ułamki tylko jednostronne. Co to znaczy? Ano jak mamy licznik i mianownik, to powinien istnieć element pierścienia R taki, że $\frac{p}{q} \cdot r$ jest znowu w R. Przecież pierścień jest nieprzemienny! Może takie r da się dobrać z jednej strony, ale z drugiej już nie? To jest możliwe. Da się na przykład skonstruować taki pierścień przy użyciu wielomianów skośnych o współczynnikach w pierścieniu funkcji wymiernych jednej zmiennej. To znowu dość duży pierścień. Ale jak wspominaliśmy wcześniej przy okazji jednostronnych odwrotności – Prawdziwe Nieprzemienne Pierścienie muszą być na swój sposób bardzo duże. W przypadku ułamków nie jest to tylko skończony wymiar. Jeśli dziedzina R nie ma z którejś strony ułamków to oznacza, że jej podpierścieniem musi być algebra wolna $Z\langle a, b\rangle$, gdzie Z – centrum R. Ta zaś jak wiadomo jest wprost monstrualnej wielkości. Jedno wiadomo na pewno. Jeżeli pierścień ma ułamki zarówno prawostronne jak i lewostronne, to są one takie same! Małe to jednak pocieszenie...

Jak widać, nieprzemienny świat najeżony jest wprost pułapkami godzącymi wprost w naszą intuicję. Jest w nim, rzecz jasna wiele pozytywnych rezultatów, nie tylko same kontrprzykłady. Teoria wielomianów skośnych, czy tzw. nieprzemiennych wyznaczników znalazła szereg zastosowań w geometrii algebraicznej, topologii algebraicznej, także fizyce czy chemii. Zainteresowanych dokładniejszymi informacjami odsyłam do moich notatek z wykładu prof. J. Matczuka o pierścieniach nieprzemiennych:

http://students.mimuw.edu.pl/ am234204/pniepnot.pdf

Dziękuję!