UNIWERSYTET WARSZAWSKI

STRUKTURY ALGEBRAICZNE

Piotr M. Hajac

28.01.2013

Jedno binarne łączne działanie

Niech G będzie niepustym zbiorem. Odwzorowanie $G \times G \ni (a, b) \mapsto ab \in G$ nazywamy łącznym działaniem $\Leftrightarrow$

$$\boxed{\forall\, a, b, c \in G \colon a(bc) = (ab)c}\,.$$

Jedno binarne łączne działanie

Niech G będzie niepustym zbiorem. Odwzorowanie $G \times G \ni (a, b) \mapsto ab \in G$ nazywamy łącznym działaniem $\Leftrightarrow$

$$\boxed{\forall\, a, b, c \in G\colon a(bc) = (ab)c}\,.$$

Struktury algebraiczne z takim działaniem są wyliczone poniżej od najbardziej do najmniej ogólnej. Każdy krok dodaje założenie, tak że każda z tych struktur jest szczególnym przypadkiem struktur powyższych.

Jedno binarne łączne działanie

Niech G będzie niepustym zbiorem. Odwzorowanie $G \times G \ni (a, b) \mapsto ab \in G$ nazywamy łącznym działaniem $\Leftrightarrow$

$$\boxed{\forall\, a, b, c \in G\colon a(bc) = (ab)c}\,.$$

Struktury algebraiczne z takim działaniem są wyliczone poniżej od najbardziej do najmniej ogólnej. Każdy krok dodaje założenie, tak że każda z tych struktur jest szczególnym przypadkiem struktur powyższych.

1. Półgrupy: bez założeń. Przykład: zbiór wszystkich skończonych wyrazów napisanych z dwóch liter (ab, ba, $abba$,...).

Jedno binarne łączne działanie

Niech G będzie niepustym zbiorem. Odwzorowanie $G \times G \ni (a, b) \mapsto ab \in G$ nazywamy łącznym działaniem $\Leftrightarrow$

$$\boxed{\forall\, a, b, c \in G \colon a(bc) = (ab)c}\,.$$

Struktury algebraiczne z takim działaniem są wyliczone poniżej od najbardziej do najmniej ogólnej. Każdy krok dodaje założenie, tak że każda z tych struktur jest szczególnym przypadkiem struktur powyższych.

1. Półgrupy: bez założeń. Przykład: zbiór wszystkich skończonych wyrazów napisanych z dwóch liter (ab, ba, $abba$,...).
2. Monoidy: $\exists\, e \in G\ \forall\, g \in G \colon eg = g = ge$.
   Przykłady: $(\mathrm{Map}(X, X), \circ, \mathrm{id})$, $(\mathbb{N}, +, 0)$.

Jedno binarne łączne działanie

Niech G będzie niepustym zbiorem. Odwzorowanie $G \times G \ni (a,b) \mapsto ab \in G$ nazywamy **łącznym działaniem** $\Leftrightarrow$

$$\boxed{\forall\, a,b,c \in G\colon a(bc) = (ab)c}\,.$$

Struktury algebraiczne z takim działaniem są wyliczone poniżej od najbardziej do najmniej ogólnej. Każdy krok dodaje założenie, tak że każda z tych struktur jest szczególnym przypadkiem struktur powyższych.

1. Półgrupy: bez założeń. Przykład: zbiór wszystkich skończonych wyrazów napisanych z dwóch liter (ab, ba, $abba$,...).
2. Monoidy: $\exists\, e \in G\ \forall\, g \in G\colon eg = g = ge$.
   Przykłady: $(\mathrm{Map}(X,X), \circ, \mathsf{id})$, $(\mathbb{N}, +, 0)$.
3. Groupy: $\forall\, g \in G\ \exists\, g^{-1} \in G\colon g^{-1}g = e = gg^{-1}$.
   Przykłady: $(\mathrm{Bij}(X,X), \circ, \mathsf{id})$, $(S_n, \circ, \mathsf{id})$.

Jedno binarne łączne działanie

Niech G będzie niepustym zbiorem. Odwzorowanie $G \times G \ni (a,b) \mapsto ab \in G$ nazywamy łącznym działaniem $\Leftrightarrow$

$$\boxed{\forall\, a,b,c \in G\colon a(bc) = (ab)c}\,.$$

Struktury algebraiczne z takim działaniem są wyliczone poniżej od najbardziej do najmniej ogólnej. Każdy krok dodaje założenie, tak że każda z tych struktur jest szczególnym przypadkiem struktur powyższych.

1. Półgrupy: bez założeń. Przykład: zbiór wszystkich skończonych wyrazów napisanych z dwóch liter (ab, ba, $abba$,...).
2. Monoidy: $\exists\, e \in G\ \forall\, g \in G\colon eg = g = ge$.
   Przykłady: $(\mathrm{Map}(X,X), \circ, \mathrm{id})$, $(\mathbb{N}, +, 0)$.
3. Groupy: $\forall\, g \in G\ \exists\, g^{-1} \in G\colon g^{-1}g = e = gg^{-1}$.
   Przykłady: $(\mathrm{Bij}(X,X), \circ, \mathrm{id})$, $(S_n, \circ, \mathrm{id})$.
4. Groupy abelowe: $\forall\, g,h \in G\colon gh = hg$.
   Przykłady: $(\mathbb{Z}, +, 0)$, $(\mathbb{Z}/n\mathbb{Z}, +, 0)$.

Dwa rozdzielne działania

Niech R będzie niepustym zbiorem z dwoma binarnymi łacznymi działaniami spełniającymi warunek rozdzielności:

$$\boxed{\forall\, r, s, t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Dwa rozdzielne działania

Niech R będzie niepustym zbiorem z dwoma binarnymi łącznymi działaniami spełniającymi warunek rozdzielności:

$$\boxed{\forall\, r, s, t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraiczne struktury z dwoma takimi działaniami są wyliczone poniżej w taki sam sposób jak poprzednio.

Dwa rozdzielne działania

Niech R będzie niepustym zbiorem z dwoma binarnymi łacznymi działaniami spełniającymi warunek rozdzielności:

$$\boxed{\forall\, r, s, t \in R\colon\ (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraiczne struktury z dwoma takimi działaniami są wyliczone poniżej w taki sam sposób jak poprzednio.

1. Pierścienie:
   $(R, +, 0)$ jest grupą abelową a $(R, \cdot, 1)$ jest monoidem.
   Przykłady: $(\mathrm{End}_{\mathbb{Z}}(G); \circ, \mathrm{id};$ punktowe $+, 0$ funkcja), gdzie $(G, +, 0)$ jest grupą abelową, pierścień macierzy $M_n(\mathbb{Z})$.

Dwa rozdzielne działania

Niech R będzie niepustym zbiorem z dwoma binarnymi łacznymi działaniami spełniającymi warunek rozdzielności:

$$\boxed{\forall\, r, s, t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraiczne struktury z dwoma takimi działaniami są wyliczone poniżej w taki sam sposób jak poprzednio.

1. Pierścienie:
   $(R, +, 0)$ jest grupą abelową a $(R, \cdot, 1)$ jest monoidem.
   Przykłady: $(\mathrm{End}_{\mathbb{Z}}(G); \circ, \mathrm{id};$ punktowe $+, 0$ funkcja), gdzie $(G, +, 0)$ jest grupą abelową, pierścień macierzy $M_n(\mathbb{Z})$.
2. Pierścienie przemienne: $\forall\, r, s \in R\colon rs = sr$.
   Przykłady: $(\mathbb{Z}/n\mathbb{Z}; \cdot, 1; +, 0)$, pierścień wielomianów $(\mathbb{Z}/n\mathbb{Z})[\mathbb{N}]$.

Dwa rozdzielne działania

Niech R będzie niepustym zbiorem z dwoma binarnymi łacznymi działaniami spełniającymi warunek rozdzielności:

$$\boxed{\forall\, r, s, t \in R\colon\ (r+s)t = rt + st,\ \ r(s+t) = rs + rt}\,.$$

Algebraiczne struktury z dwoma takimi działaniami są wyliczone poniżej w taki sam sposób jak poprzednio.

1. Pierścienie:
   $(R, +, 0)$ jest grupą abelową a $(R, \cdot, 1)$ jest monoidem.
   Przykłady: $(\mathrm{End}_{\mathbb{Z}}(G); \circ, \text{id};$ punktowe $+, 0$ funkcja), gdzie $(G, +, 0)$ jest grupą abelową, pierścień macierzy $M_n(\mathbb{Z})$.
2. Pierścienie przemienne: $\forall\, r, s \in R\colon\ rs = sr$.
   Przykłady: $(\mathbb{Z}/n\mathbb{Z}; \cdot, 1; +, 0)$, pierścień wielomianów $(\mathbb{Z}/n\mathbb{Z})[\mathbb{N}]$.
3. Pierścienie całkowite $rs = 0 \Rightarrow (r = 0$ lub $s = 0)$.
   Examples: $(\mathbb{Z}; \cdot, 1; +, 0)$, pierścień wielomianów $\mathbb{Z}[\mathbb{N}]$.

Dwa rozdzielne działania

Niech R będzie niepustym zbiorem z dwoma binarnymi łącznymi działaniami spełniającymi warunek rozdzielności:

$$\boxed{\forall\, r, s, t \in R\colon\ (r+s)t = rt + st,\ \ r(s+t) = rs + rt}\ .$$

Algebraiczne struktury z dwoma takimi działaniami są wyliczone poniżej w taki sam sposób jak poprzednio.

1. Pierścienie:
   $(R, +, 0)$ jest grupą abelową a $(R, \cdot, 1)$ jest monoidem.
   Przykłady: $(\mathrm{End}_{\mathbb{Z}}(G); \circ, \mathrm{id};$ punktowe $+, 0$ funkcja), gdzie $(G, +, 0)$ jest grupą abelową, pierścień macierzy $M_n(\mathbb{Z})$.
2. Pierścienie przemienne: $\forall\, r, s \in R\colon rs = sr$.
   Przykłady: $(\mathbb{Z}/n\mathbb{Z}; \cdot, 1; +, 0)$, pierścień wielomianów $(\mathbb{Z}/n\mathbb{Z})[\mathbb{N}]$.
3. Pierścienie całkowite $rs = 0 \Rightarrow (r = 0$ lub $s = 0)$.
   Examples: $(\mathbb{Z}; \cdot, 1; +, 0)$, pierścień wielomianów $\mathbb{Z}[\mathbb{N}]$.
4. Ciała: $(R \setminus \{0\}, \cdot, 1)$ jest grupą.
   Przykłady: $(\mathbb{Z}/p\mathbb{Z}; \cdot, 1; +, 0)$, gdzie p jest liczbą pierwszą.

Dwa rozdzielne działania

Niech R będzie niepustym zbiorem z dwoma binarnymi łacznymi działaniami spełniającymi warunek rozdzielności:

$$\boxed{\forall\, r, s, t \in R\colon (r+s)t = rt + st,\ r(s+t) = rs + rt}\,.$$

Algebraiczne struktury z dwoma takimi działaniami są wyliczone poniżej w taki sam sposób jak poprzednio.

1. Pierścienie:
   $(R, +, 0)$ jest grupą abelową a $(R, \cdot, 1)$ jest monoidem.
   Przykłady: $(\mathrm{End}_{\mathbb{Z}}(G); \circ, \mathrm{id};$ punktowe $+, 0$ funkcja), gdzie $(G, +, 0)$ jest grupą abelową, pierścień macierzy $M_n(\mathbb{Z})$.
2. Pierścienie przemienne: $\forall\, r, s \in R\colon rs = sr$.
   Przykłady: $(\mathbb{Z}/n\mathbb{Z}; \cdot, 1; +, 0)$, pierścień wielomianów $(\mathbb{Z}/n\mathbb{Z})[\mathbb{N}]$.
3. Pierścienie całkowite $rs = 0 \Rightarrow (r = 0$ lub $s = 0)$.
   Examples: $(\mathbb{Z}; \cdot, 1; +, 0)$, pierścień wielomianów $\mathbb{Z}[\mathbb{N}]$.
4. Ciała: $(R \setminus \{0\}, \cdot, 1)$ jest grupą.
   Przykłady: $(\mathbb{Z}/p\mathbb{Z}; \cdot, 1; +, 0)$, gdzie p jest liczbą pierwszą.
5. Ciała o charakterytyce 0: zawierają $\mathbb{Q}$ jako podciało.
   Przykłady: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Rozdzielne działania na grupach abelowych

Niech M będzie grupą abelową a R pierścieniem wyposażonymi w łączne działanie:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M}\,.$$

Rozdzielne działania na grupach abelowych

Niech M będzie grupą abelową a R pierścieniem wyposażonymi w łączne działanie:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M} \, .$$

Takie struktury algebraiczne są opisane poniżej w taki sam sposób jak poprzednio.

Rozdzielne działania na grupach abelowych

Niech M będzie grupą abelową a R pierścieniem wyposażonymi w łączne działanie:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M}\ .$$

Takie struktury algebraiczne są opisane poniżej w taki sam sposób jak poprzednio.

1. Moduły: $\forall\, m, n \in M, r, s \in R$:
   $(r+s)m = rm + sm,\ r(m+n) = rm + rn,\ 1m = m$.
   Przykłady: $\mathrm{End}_{\mathbb{Z}}(G) \times G \ni (f, g) \mapsto f(g) \in G$
   oraz $\mathbb{Z}^n$ nad pierścieniem macierzy $M_n(\mathbb{Z})$.

Rozdzielne działania na grupach abelowych

Niech M będzie grupą abelową a R pierścieniem wyposażonymi w łączne działanie:

$$\boxed{R \times M \ni (r,m) \longmapsto rm \in M}\ .$$

Takie struktury algebraiczne są opisane poniżej w taki sam sposób jak poprzednio.

1. Moduły: $\forall\ m, n \in M, r, s \in R$:
   $(r+s)m = rm + sm,\ r(m+n) = rm + rn,\ 1m = m.$
   Przykłady: $\mathrm{End}_{\mathbb{Z}}(G) \times G \ni (f,g) \mapsto f(g) \in G$ oraz $\mathbb{Z}^n$ nad pierścieniem macierzy $M_n(\mathbb{Z})$.
2. Wolne moduły: istnieje baza M. Przykład: $\bigoplus_{\mathbb{N}} R$.

Rozdzielne działania na grupach abelowych

Niech M będzie grupą abelową a R pierścieniem wyposażonymi w łączne działanie:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M}\ .$$

Takie struktury algebraiczne są opisane poniżej w taki sam sposób jak poprzednio.

1. Moduły: $\forall\ m, n \in M, r, s \in R$:
   $(r+s)m = rm + sm,\ r(m+n) = rm + rn,\ 1m = m$.
   Przykłady: $\mathrm{End}_{\mathbb{Z}}(G) \times G \ni (f, g) \mapsto f(g) \in G$
   oraz $\mathbb{Z}^n$ nad pierścieniem macierzy $M_n(\mathbb{Z})$.
2. Wolne moduły: istnieje baza M. Przykład: $\bigoplus_{\mathbb{N}} R$.
3. Przestrzenie wektorowe: R jest ciałem. Przykład: $\bigoplus_{\mathbb{N}} R$.

Rozdzielne działania na grupach abelowych

Niech M będzie grupą abelową a R pierścieniem wyposażonymi w łączne działanie:

$$\boxed{R \times M \ni (r, m) \longmapsto rm \in M}\ .$$

Takie struktury algebraiczne są opisane poniżej w taki sam sposób jak poprzednio.

1. Moduły: $\forall\ m, n \in M, r, s \in R$:
   $(r + s)m = rm + sm,\ r(m + n) = rm + rn,\ 1m = m.$
   Przykłady: $\mathrm{End}_{\mathbb{Z}}(G) \times G \ni (f, g) \mapsto f(g) \in G$
   oraz $\mathbb{Z}^n$ nad pierścieniem macierzy $M_n(\mathbb{Z})$.
2. Wolne moduły: istnieje baza M. Przykład: $\bigoplus_{\mathbb{N}} R$.
3. Przestrzenie wektorowe: R jest ciałem. Przykład: $\bigoplus_{\mathbb{N}} R$.
4. Skończeniewymiarowe przestrzenie wektorowe: istnieje baza skończona M. Przykład: R^n.

Algebry nad przemiennymi pierścieniami

Niech A będzie modułem nad przemiennym pierścieniem k wyposażonym w k-biliniowe łączne mnożenie

$$\boxed{A \times A \ni (a, b) \longmapsto ab \in A}\,.$$

Wtedy A nazywa się algebrą nad k.

Algebry nad przemiennymi pierścieniami

Niech A będzie modułem nad przemiennym pierścieniem k wyposażonym w k-biliniowe łączne mnożenie

$$\boxed{A \times A \ni (a, b) \longmapsto ab \in A}\,.$$

Wtedy A nazywa się algebrą nad k.

Mówimy że algebra A jest algebrą z jedynką wtedy i tylko wtedy gdy A jest pierścieniem ze względu na swoją strukturę grupy abelowej i mnożenie. Innymi słowy, algebra z jedynką to moduł z liniową strukturą pierścienia, lub pierścień ze zgodną strukturą modułu. Każdy pierścień jest algebrą z jedynką nad pierścieniem $\mathbb{Z}$ wszystkich liczb całkowitych.

Spektrum, wektory i wartości własne

Niech A będzie algebrą z jedynką nad przemiennym pierścieniem k. Spectrum elementu $a \in A$ to następujący podzbiór k:

$$\boxed{\operatorname{spec}_A(a) := \{\lambda \in k \mid \nexists\, (a - \lambda 1)^{-1} \in A\}}\,.$$

Spektrum, wektory i wartości własne

Niech A będzie algebrą z jedynką nad przemiennym pierścieniem k. Spectrum elementu $a \in A$ to następujący podzbiór k:

$$\boxed{\mathrm{spec}_A(a) := \{\lambda \in k \mid \nexists\, (a - \lambda 1)^{-1} \in A\}}\,.$$

W szczególności, gdy M jest modułem nad k, możemy wziąć $A = \mathrm{End}_k(M)$. Wówczas element $v \in M$ nazywany jest wektorem własnym endomorfizmu $a \in \mathrm{End}_k(M)$ przynależącym do $\lambda \in k$ wtedy i tylko wtedy gdy $av = \lambda v$. Zauważmy że $v \neq 0 \Rightarrow \lambda \in \mathrm{spec}_A(a)$. Wszystkie elementy $\mathrm{spec}_A(a)$ pochodzące od niezerowych wektorów własnych endomorfizmu a nazywamy wartościami własnymi.

Spektrum, wektory i wartości własne

Niech A będzie algebrą z jedynką nad przemiennym pierścieniem k. Spectrum elementu $a \in A$ to następujący podzbiór k:

$$\boxed{\mathrm{spec}_A(a) := \{\lambda \in k \mid \ \nexists\, (a - \lambda 1)^{-1} \in A\}}\ .$$

W szczególności, gdy M jest modułem nad k, możemy wziąć $A = \mathrm{End}_k(M)$. Wówczas element $v \in M$ nazywany jest wektorem własnym endomorfizmu $a \in \mathrm{End}_k(M)$ przynależącym do $\lambda \in k$ wtedy i tylko wtedy gdy $av = \lambda v$. Zauważmy że $v \neq 0 \ \Rightarrow \lambda \in \mathrm{spec}_A(a)$. Wszystkie elementy $\mathrm{spec}_A(a)$ pochodzące od niezerowych wektorów własnych endomorfizmu a nazywamy wartościami własnymi.

Jeśli M jest skończeniewymiarowym wolnym modułem nad niezerowym przemiennym pierścieniem k, to wszystkie elementy spektrum dowolnego endemorfizmu a są wartościami własnymi. Są one pierwiastkami wielomianu charakterystycznego

$$\boxed{\det(a - \lambda\,\mathsf{id})}\ .$$