Metody algebry liniowej w fizyce

Elżbieta Adamus
Wydział Matematyki Stosowanej
Akademia Górniczo-Hutnicza w Krakowie

Kraków 2024

References

[1] Z. Furdzik, J. Maj-Kluskowa, A. Kulczycka, M. Sękowska, *Nowoczesna matematyka dla inżynierów. Część I - Algebra*, Wydawnictwo AGH, Kraków, 1993

[2] B. Gleichgewicht, *Algebra*, PWN, Warszawa, 1983, wydanie III zmienione

[3] T. Jurlewicz, Z. Skoczylas, *Algebra i geometria analityczna. Definicje, twierdzenia, wzory*, Oficyna Wydawnicza GiS, Wrocław, 2020, wydanie XXII

[4] T. Jurlewicz, Z. Skoczylas, *Algebra liniowa. Definicje, twierdzenia, wzory*, Oficyna Wydawnicza GiS, Wrocław, 2015, wydanie VIII poprawione

[5] A. I. Kostrikin, *Wstęp do algebry, tomy 1,2*, Wydawnictwo Naukowe PWN, 2004.

Elżbieta Adamus
Wydział Matematyki Stosowanej
Akademia Górniczo-Hutnicza w Krakowie

Algebra
Wykład nr 1
Data: .....

TEMAT: *Działania i wybrane struktury algebraiczne*

1.1 Notacja

Przyjmujemy następująca notację.

$\mathbb{N} = \{1, 2, 3, \ldots\}$	zbiór liczb naturalnych
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$	
$\mathbb{Z}$	zbiór liczb całkowitych
$\mathbb{Q}$	zbiór liczb wymiernych
$\mathbb{R}$	zbiór liczb rzeczywistych

Oznaczenia kwantyfikatorów

$\forall$	kwantyfikator ogólny (duży)	*dla każdego*
$\exists$	kwantyfikator szczegółowy (mały)	*istnieje*
$\exists!$		*istnieje dokładnie jeden*

Symbol sumy i iloczynu

Niech $n \in \mathbb{N}$ oraz niech $a_1, a_2, \ldots, a_m, a_{m+1}, \ldots, a_n$ to dowolny ciąg liczb.

Sumę $a_1 + a_2 + \ldots + a_n$ oznaczamy symbolem $\sum_{i=1}^{n} a_i$. Symbol i to wskaźnik sumowania lub indeks sumowania, m to dolna granica sumowania, zaś n to górna granica sumowania.

Zauważmy że dla dowolnego $m \in \mathbb{N}$, $m < n$ oraz $c \in \mathbb{R}$ zachodzą równości
$a_1 + a_2 + \ldots + a_n = (a_1 + a_2 + \ldots + a_m) + (a_{m+1} + a_{m+2} + \ldots + a_n)$ oraz
$c(a_1 + a_2 + \ldots + a_n) = ca_1 + ca_2 + \ldots + ca_n$, czyli

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{m} a_i + \sum_{i=m+1}^{n} a_i, \qquad c\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} ca_i.$$

Przykład 1.1.1. $\sum_{i=1}^{6} i = 1 + 2 + 3 + 4 + 5 + 6 = 21$
$\sum_{i=5}^{9} \frac{i}{i+2} = \frac{5}{7} + \frac{6}{8} + \frac{7}{9} + \frac{8}{10} + \frac{9}{11}$
$\sum_{i=0}^{n} \left(\frac{1}{2}\right)^i = 1 + \frac{1}{2} + \frac{1}{4} + \ldots + \left(\frac{1}{2}\right)^n = \frac{1-\left(\frac{1}{2}\right)^{n+1}}{1-\frac{1}{2}}$

Iloczyn $a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} \cdot a_n$ oznaczamy symbolem $\prod_{i=1}^{n} a_i$. Symbol i to wskaźnik iloczynu, m to dolny wskaźnik iloczynu, zaś n to górny wskaźnik iloczynu.

Przykład 1.1.2. $\prod_{i=0}^{6}(9-j) = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$
$\prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (-1) \cdot n = n!$
$\underbrace{x \cdot x \cdot \ldots \cdot x}_{n\ razy} = \prod_{i=1}^{n} x$

1.2 Działania wewnętrzne i ich własności

Niech A będzie zbiorem niepustym.

Definicja 1.2.1. Dowolną funkcję $h : A \times A \to A$ nazywamy *działaniem wewnętrznym* w zbiorze A. Wartość funkcji $h(a, b) \in A$ nazywamy *wynikiem* działania dla pary argumentów $a, b \in A$.

Przykład 1.2.2. i) Dodawanie jest działaniem wewnętrznym w $\mathbb{N}$.

ii) Odejmowanie nie jest działaniem wewnętrznym w $\mathbb{N}$.

iii) Dodawanie nie jest działaniem wewnętrznym w $\mathbb{R} \setminus \mathbb{Q}$.

Własności działań wewnętrznych

Definicja 1.2.3. Niech $* : A \times A \to A$ będzie działaniem wewnętrznym.

i) Działanie $*$ nazywamy *przemiennym*, jeśli $\forall\, a, b \in A \quad a * b = b * a$.

ii) Działanie $*$ nazywamy *łącznym*, jeśli $\forall\, a, b, c \in A \quad (a * b) * c = a * (b * c)$.

iii) Element $e \in A$ nazywamy *elementem neutralnym* działania $*$, jeśli $\forall\, a \in A \quad a * e = e * a = a$.

Przykład 1.2.4. i) Dodawanie jest działaniem wewnętrznym łącznym i przemiennym w $\mathbb{R}$. 0 jest elementem neutralnym.

ii) Mnożenie jest działaniem wewnętrznym łącznym i przemiennym w $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. 1 jest elementem neutralnym.

Twierdzenie 1.2.5. Jeżeli element neutralny istnieje to jest jedyny.

Dowód. Przypuśćmy, że istnieją $e_1, e_2 \in A$ będące elementami neutralnymi w A. Wówczas $e_2 = e_1 * e_2 = e_1$. $\square$

Przykład 1.2.6. Niech X to dowolny zbiór.

i) Zbiór pusty $\varnothing$ jest elementem neutralnym w $\big(P(X), \cup\big)$.

ii) Zbiór X jest elementem neutralnym w $\big(P(X), \cap\big)$.

Definicja 1.2.7. Niech $* : A \times A \to A$ będzie działaniem wewnętrznym, posiadającym element neutralny $e \in A$. Dla dowolnego $a \in A$ każdy element $a' \in A$ taki, że $a * a' = a' * a = e$, nazywamy *elementem symetrycznym* do a względem działania $*$.

Przykład 1.2.8. i) W $(\mathbb{R}, +)$ elementem symetrycznym do 5 jest -5 (tzw. element przeciwny).

ii) W $(\mathbb{R}^*, \cdot)$ elementem symetrycznym do 5 jest $\frac{1}{5}$ (tzw. element odwrotny).

iii) W $(\mathbb{R}, \circ)$, gdzie $x \circ y = x + y + 1$, elementem neutralnym jest -1, zaś elementem symetrycznym do x jest $-2 - x$.

Twierdzenie 1.2.9. Jeżeli działanie wewnętrzne jest łączne oraz posiada element neutralny, to każdy element posiada co najwyżej jeden element symetryczny.

Dowód. Rozważmy zbiór A z działaniem łącznym $\circ$. Niech e będzie elementem neutralnym działania $\circ$. Niech a', a'' to dwa elementy symetryczne do $a \in A$. Wówczas

$$\begin{aligned} a \circ a' = e \;\Rightarrow\; a'' \circ (a \circ a') &= a'' \circ e \\ (a'' \circ a) \circ a' &= a'' \\ e \circ a' &= a'' \\ a' &= a'' \end{aligned}$$

□

1.3 Podstawowe struktury algebraiczne

Niech G będzie zbiorem niepustym, zaś $* : G \times G \to G$ działaniem wewnętrznym w G.

Definicja 1.3.1. i) Parę $(G, *)$ nazywamy *półgrupą*, jeżeli działanie jest łączne.

ii) Parę $(G, *)$ nazywamy *monoidem*, jeżeli działanie jest łączne i posiada element neutralny.

iii) Parę $(G, *)$ nazywamy *grupą*, jeżeli działanie jest łączne, posiada element neutralny oraz każdy element G posiada element symetryczny względem $*$ w G.

Jeśli dodatkowo działanie $*$ jest przemienne, to mówimy o *półgrupie przemiennej, monoidzie przemiennym, grupie przemiennej (abelowej).*

Przykład 1.3.2. Oznaczmy $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

	$(\mathbb{N},+)$	$(\mathbb{Z},\cdot)$	$(\mathbb{Q},+)$	$(\mathbb{Q},\cdot)$	$(\mathbb{R}^*,+)$	$(\mathbb{R}^*,\cdot)$
wewnętrzność	✓	✓	✓	✓	nie $-1+1=0$ $0\notin\mathbb{R}^*$	✓
łączność	✓	✓	✓	✓		✓
przemienność	✓	✓	✓	✓		✓
el. neutralny	brak $0\notin\mathbb{N}$	✓ $1\in\mathbb{Z}$	✓ $0\in\mathbb{Q}$	✓ $1\in\mathbb{Q}$		✓ $1\in\mathbb{R}^*$
el. symetryczny		brak $2\cdot b=1$ $b=\frac{1}{2}\notin\mathbb{Z}$	✓ $a+a'=0$ $a'=-a\in\mathbb{Q}$	brak $a\cdot a'=1$ $a'=\frac{1}{a}$ nie dla $a=0$		✓ $a\cdot a'=1$ $a'=\frac{1}{a}$ $\forall a\in\mathbb{R}^*$
	półgrupa przemienna bez el. neutr.	monoid przemienny	grupa abelowa	monoid przemienny		grupa abelowa

Przykład 1.3.3. Niech $X=\{1,2,4,\ldots,2^n,\ldots\}$, $n\in\mathbb{N}_0=\mathbb{N}\cup\{0\}$, zaś działanie $\circ$ to mnożenie liczb. Czy $(X,\circ)$ jest półgrupą/grupą (abelową)?

Jeśli $a,b,c\in X$, to istnieją $k,m,n\in\mathbb{N}_0$ takie, ze $a=2^n, b=2^m, c=2^k$.

wewnętrzne $\quad a\circ b=2^n\cdot 2^m=2^{n+m}\in A$

przemienne $\quad a\circ b=2^n\cdot 2^m=2^{n+m}=2^{m+n}=2^m\cdot 2^n=b\circ a$

łączne $\quad (a\circ b)\circ c=2^{n+m}\cdot 2^k=2^{n+m+k}=2^n\cdot 2^{m+k}=a\circ(b\circ c)$

el. neutralny $\quad e=2^s, s\in\mathbb{N}_0 \quad a\circ e=a \Leftrightarrow 2^{n+s}=2^n \Rightarrow s=0,\ e=1\in X$

brak el. odwrotnego $\quad a\circ b=1 \Leftrightarrow 2^{n+m}=2^0 \Leftrightarrow m=-n \Rightarrow m=-n\notin\mathbb{N}_0$

Wniosek: monoid przemienny (tj. półgrupa przemienna z jedynką)

Definicja 1.3.4. Zespół $(A,\circ,*)$ złożony z niepustego zbioru A i określonych w nim działań wewnętrznych $\circ: A\times A\to A$, $*: A\times A\to A$ nazywamy *pierścieniem*, jeśli $(A,\circ)$ jest grupą abelową, zaś działanie $*$ jest łączne oraz rozdzielne względem działania $\circ$, tzn.

$$\forall a,b,c\in A \quad (a\circ b)*c=(a*c)\circ(b*c) \ \wedge\ c*(a\circ b)=(c*a)\circ(c*b).$$

Pierścień, w którym działanie $*$ posiada element neutralny, nazywamy *pierścieniem z jedynką* lub *z jednością*. Pierścień, w którym działanie $*$ jest przemienne, nazywamy *pierścieniem przemiennym* lub *komutatywnym*.

	Notacja addytywna		Notacja multiplikatywna
$\circ\,/\,+$	dodawanie	$*\,/\,\cdot$	mnożenie
$a+b$	suma	$a\cdot b$	iloczyn
$e=0$	zero	$e=1$	jedynka
$a'=-a$	element przeciwny	$a'=a^{-1}$	element odwrotny

	$na=\underbrace{a+\ldots+a}_{n},\ n\in\mathbb{N}$	$a^n=\underbrace{a\cdot\ldots\cdot a}_{n}$
	$0\cdot a=0$	$a^0=e=e=1$
$m\in\mathbb{Z}, m<0$	$ma=\underbrace{(-a)+\ldots+(-a)}_{m}$	$a^m=\underbrace{a^{-1}\cdot\ldots\cdot a^{-1}}_{n}$

Definicja 1.3.5. Zespół $(K,\circ,*)$ złożony ze zbioru K zawierającego co najmniej dwa elementy i określonych w nim działań wewnętrznych $\circ : K\times K\to K$, $* : K\times K\to K$ nazywamy *ciałem*, jeśli

- $(K,\circ)$ jest grupą abelową (z elementem neutralnym $e_\circ$),
- $(K\setminus\{e_\circ\},*)$ jest grupą abelową,
- działanie $*$ jest rozdzielne względem działania $\circ$.

Zatem ciało to pierścień przemienny z jedynką (różną od zera, tj. $1=e_*\neq e_\circ=0$), w którym wszystkie niezerowe (tj. różne od elementu neutralnego $e_\circ$) elementy są odwracalne.

Zatem w ciele można zdefiniować operację *dzielenia* w sposób następujący:

$$\frac{a}{b}:=a*b^{-1},\quad a,b\in K,\ b\neq 0.$$

Przykład 1.3.6. i) $(\mathbb{R},+,\cdot)$ ciało liczb rzeczywistych
$(\mathbb{R},+)$ grupa addytywna ciała
$(\mathbb{R}^*,\cdot)$ grupa multiplikatywna ciała

ii) $(\mathbb{Q},+,\cdot)$ ciało liczb wymiernych

iii) $(\mathbb{Z},+,\cdot)$ pierścień przemienny z jedynką, ale nie ciało (bowiem np. $2^{-1}\notin\mathbb{Z}$)

iv) $(\mathbb{Z}/p\mathbb{Z},+_p,\cdot_p)$, gdzie $p\in\mathbb{N}$, $p\geq 2$
$+_p,\cdot_p$ dodawanie i mnożenie modulo p

Jeśli p to liczba pierwsza, to $\mathbb{Z}/p\mathbb{Z}$ jest ciałem (tzw. ciało reszt modulo p). Jeśli p nie jest liczbą pierwszą, to $\mathbb{Z}/p\mathbb{Z}$ jest pierścieniem, ale nie ciałem.

$\mathbb{Z}/5\mathbb{Z}$ to ciało

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}/4\mathbb{Z}$ nie jest ciałem

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Definicja 1.3.7. Niech $(A, +, \cdot)$ będzie pierścieniem. Elementy $a, b \in A, a \neq 0, b \neq 0$ nazywamy *dzielnikami zera*, jeśli $a \cdot b = 0$.

Uwaga 1.3.8. W ciele nie ma dzielników zera.

Dowód. Niech $(K, +, \cdot)$ będzie ciałem oraz niech $a, b \in K$. Załóżmy, że $a \cdot b = 0$ oraz $a \neq 0$. Jeśli $a \neq 0$, to istnieje $a^{-1} \in K$. Otrzymujemy

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b_{=}(a^{-1} \cdot a) \cdot b = 1 \cdot b = b.$$

Zatem $b = 0$. $\square$

Przykład 1.3.9. Sprawdź, że zbiór $\mathbb{R}^2$ wraz z działaniami dodawania i mnożenia zdefiniowanymi poniżej ma strukturę ciała.

$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 \quad (x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2),\ (x_1, y_1) \cdot (x_2, y_2) := (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1).$

$(\mathbb{C}, +)$ jest grupą abelową.

Działanie $+$ jest wewnętrzne, łączne, przemienne. Elementem neutralnym jest $(0, 0) \in \mathbb{R}^2$, zaś elementem przeciwnym do $(x_1, y_1) \in \mathbb{R}^2$ jest $(-x_1, -y_1) \in \mathbb{R}^2$.

$(\mathbb{C} \setminus \{(0, 0)\}, \cdot)$ jest grupą abelową.

Działanie $\cdot$ jest wewnętrzne.

przemienność:

$$(x_2, y_2) \cdot (x_1, y_1) = (x_2 x_1 - y_2 y_1, x_2 y_1) = \ = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) = (x_1, y_1) \cdot (x_2, y_2)$$

łączność: $L = P$

$$L = (a,b)\cdot[(x_1,y_1)\cdot(x_2,y_2)] = (a,b)\cdot(x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) =$$
$$= (ax_1x_2 - ay_1y_2 - bx_1y_2 - bx_2y_1, ax_1y_2 + ax_2y_1 + bx_1x_2 - by_1y_2)$$
$$P = [(a,b)\cdot(x_1,y_1)]\cdot(x_2,y_2) = (ax_1 - by_1, ay_1 + bx_1)\cdot(x_2,y_2) =$$
$$= (ax_1x_2 - by_1x_2 - ay_1y_2 - bx_1y_2, ax_1y_1 - by_1y_2 + ay_1x_2 + bx_1x_2)$$

el. neutralny: $e = (1,0)$

$$\forall(x_1,y_1)\in\mathbb{R}^2 \quad (1,0)\cdot(x_1,y_1) = (1\cdot x_1 - 0\cdot y_1, 1\cdot y_1 + 0\cdot x_1) = (x_1,y_1)$$

el. odwrotny do $(x_1,y_1)\neq(0,0)$:

$$(x_1,y_1)\cdot(a,b) = (1,0) \Leftrightarrow (ax_1 - by_1, ay_1 + bx_1) = (1,0) \Leftrightarrow \begin{bmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{bmatrix}\cdot\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

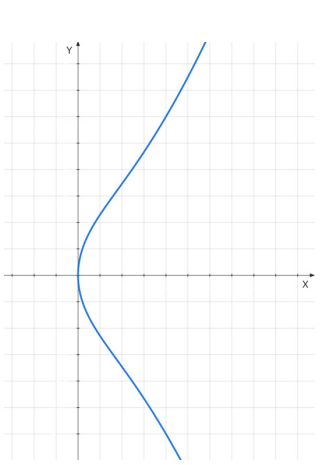
$$\forall(x_1,y_1)\neq(0,0) \quad a = \frac{x_1}{x_1^2+y_1^2},\ b = \frac{y_1}{x_1^2+y_1^2}$$

Działanie $\cdot$ jest rozdzielne względem $+$, bowiem $L = P$.

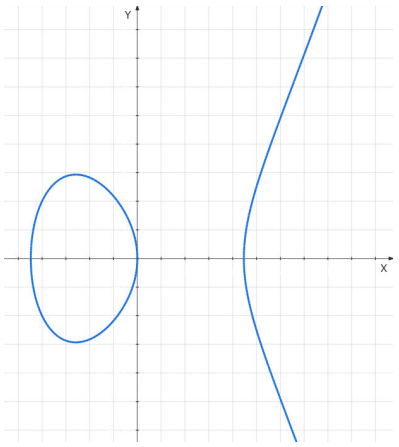
$$L = (a,b)\cdot[(x_1,y_1)+(x_2,y_2)] = (a,b)\cdot(x_1+x_2,y_1+y_2) = (ax_1+ax_2-by_1-by_2, ay_1+ay_2+bx_1+bx_2)$$
$$P = [(a,b)\cdot(x_1,y_1)] + [(a,b)\cdot(x_2,y_2)] = (ax_1 - by_1, ay_1 + bx_1) + (ax_2 - by_2, ay_2 + bx_2)$$

Definicja 1.3.10. Zdefiniowane powyżej ciało nazywamy *ciałem liczb zespolonych* i oznaczamy symbolem $\mathbb{C}$. Elementy tego ciała nazywamy *liczbami zespolonymi*.

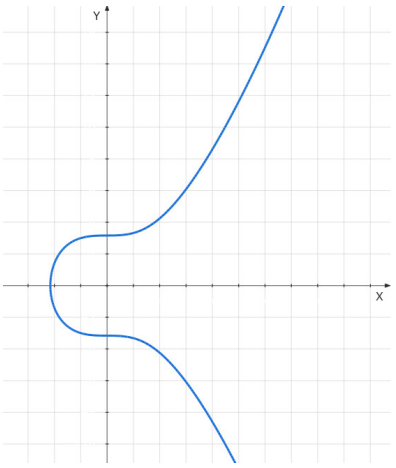
Przykład 1.3.11 (Struktura grupy na krzywej eliptycznej)**.** Niech $K = \mathbb{R}$ lub $K = \mathbb{C}$. *Krzywą eliptyczną* nad ciałem K nazywamy krzywą zdefiniowaną równaniem $y^2 = x^3 + ax + b$, gdzie $a, b \in K$ są takie, że $4a^3 + 27b^2 \neq 0$.
Warunek ten zapewnia, iż krzywa nie ma punktów osobliwych.



$y^2 = x^3 + 20x$ nad $\mathbb{R}$



$y^2 = x^3 - 20x$ nad $\mathbb{R}$



$y^2 = x^3 + 10$ nad $\mathbb{R}$

Oznaczmy

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

gdzie $\mathcal{O}$ jest pewnym wyróżnionym punktem, zwanym *punktem w nieskończoności*.

W zbiorze $E(K)$ można zdefiniować operację grupową $+$ „dodawania" punktów, dla której $\mathcal{O}$ jest elementem neutralnym i taką, że $(E(K), +)$ jest grupą abelową.

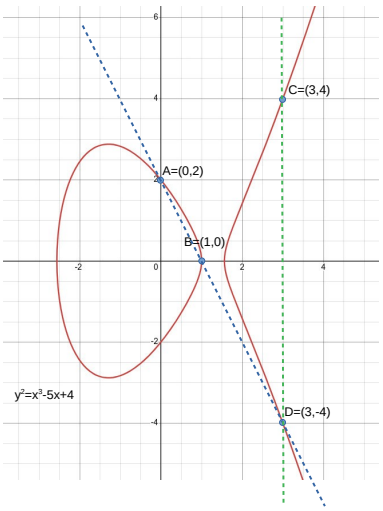
Niech $A = (x_1, y_1), B = (x_2, y_2)$ to dwa punkty ze zbioru $E(K)$. Zdefinujemy działanie $+ : E(K) \times E(K) \to E(K)$ w opisany niżej sposób.

1. $A + \mathcal{O} = A$, $\mathcal{O} + B = B$
2. Jeśli $x_1 = x_2$ oraz $y_1 = -y_1$, wówczas $A + B = \mathcal{O}$.
3. W pozostałych przypadkach obliczamy $\lambda = \begin{cases} \frac{3x_1^2+a}{2y_1} & ; \quad A = B \\ \frac{y_1-y_2}{x_1-x_2} & : \quad A \neq B \end{cases}$.

Wówczas $A + B = C = (x_3, y_3)$, gdzie $x_3 = \lambda^2 - x_1 - x_2$ oraz $y_3 = -\lambda x_3 - \nu$, dla $\nu = y_1 - \lambda x_1$.

W przypadku gdy $A \neq B$ oraz $x_1 \neq x_2$ dodawanie punktów można opisać geometrycznie w następujący sposób.

Wyznaczmy prostą l przechodzącą przez punkty A i B. Można wykazać, że wówczas prosta l przecina krzywą w dokładnie trzech punktach A, B oraz $D = (x_4, y_4)$, gdzie $x_3 = \lambda^2 - x_1 - x_2$ oraz $y_3 = \lambda x_3 + \nu$, dla $\nu = y_1 - \lambda x_1$. Inaczej mówiąc $x_4 = x_3$ zaś $y_4 = -y_3$.



Krzywe eliptyczne znajdują zastosowanie w kryptografii. Więcej informacji można znaleźć tutaj lub tutaj.