12. ROZSZERZENIE CIAŁA O ELEMENT ALGEBRAICZNY

Wspominaliśmy poprzednio o ciele złożonym z liczb $a+b\sqrt{2}$, gdzie a, b są liczbami wymiernymi. Jest to rozszerzenie ciała liczb wymiernych Q, przy czym jest to najmniejsze ciało zawierające wszystkie liczby wymierne oraz liczbę $\sqrt{2}$. Istotnie, każde ciało zawerające liczby wymierne a, b oraz liczbę $\sqrt{2}$ zawiera liczbę $a+b\sqrt{2}$.

Przypuśćmy, że jest ustalone ciało K i pewien element a algebraiczny względem ciała K. Niech L będzie pewnym ustalonym rozszerzeniem ciała K zawierającym element a. Wyjaśnimy, z jakich elementów składa się najmniejsze podciało ciała L zawierające ciało K oraz element a.

Przypuśćmy, że a jest elementem algebraicznym stopnia n względem ciała K. Niech

$$f = a_n x^n + \ldots + a_0$$

będzie wielomianem minimalnym elementu a.

W każdym ciele są wykonalne działania dodawania, odejmowania, mnożenia, dzielenia (przez elementy różne od zera), zatem każde rozszerzenie ciała K zawiera wszystkie elementy mające postać

$$c_0 + c_1 a + c_2 a^2 + \ldots + c_k a^k$$

gdzie $c_i \in K$. Okazuje się, że można ograniczyć się do wykładników k mniejszych od n. Jeśli bowiem $k \geqslant n$, to rozważmy następujący wielomian

$$g = c_0 + c_1 x + c_2 x^2 + \ldots + c_k x^k$$

wyznaczmy iloraz i resztę z dzielenia tego wielomianu przez f

$$g = q \cdot f + r$$

przy czym

$r = d_0 + d_1 x + \ldots + d_{n-1} x^{n-1}, \quad d_i \in K$

ponieważ reszta jest wielomianem stopnia mniejszego niż dzielnik. Dla $x = a$

$g(a) = q(a) \cdot f(a) + r(a)$

ponieważ $f(a) = 0$, więc

$g(a) = r(a)$

to znaczy, że

$c_0 + c_1 a + \ldots + c_k a^k = d_0 + d_1 a + \ldots + d_{n-1} a^{n-1}$

Wykażemy, że zbiór elementów o postaci

$c_0 + c_1 a + \ldots + c_{n-1} a^{n-1}$

stanowi podciało ciała L. Wystarczy stwierdzić, że różnica oraz iloraz elementów mających tę postać też są elementami tej postaci. W przypadku różnicy jest to oczywiste

$(c_0 + c_1 a + \ldots + c_{n-1} a^{n-1}) - (d_0 + d_1 a + \ldots d_{n-1} a^{n-1}) =$

$(c_0 - d_0) + (c_1 - d_1) a + \ldots + (c_{n-1} - d_{n-1}) a^{n-1}$

Aby udowodnić, że iloraz dwóch wyrażeń o rozważanej postaci też ma tę postać, wystarczy stwierdzić, że jeśli

$c_0 + c_1 a + \ldots + c_{n-1} a^{n-1} \neq 0$

to

$(c_0 + c_1 a + \ldots + c_{n-1} a^{n-1})^{-1}$

też jest elementem o takiej postaci.
Niech

$g = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$

Oczywiście stopień wielomianu g jest liczbą większą od zera i mniejszą od n. Wobec nierozkładalności wielomianu minimalnego f wielomiany f i g są względnie pierwsze, a zatem ([6], str. 180 twierdzenie 12) istnieją wielomiany φ, ψ, dla których

$1 = \varphi \cdot f + \psi \cdot g$

Wobec tego

$\varphi(a) \cdot f(a) + \psi(a) \cdot g(a) = 1$

Ponieważ $f(a) = 0$, więc

$\psi(a) \cdot g(a) = 1$

to znaczy, że

$(c_0 + c_1 a + \ldots + c_{n-1} a^{n-1})^{-1} = \psi(a)$

Element $\psi(a)$ ma postać

$d_0 + d_1 a + \ldots + d_k a^k$

przy czym, jak stwierdziliśmy wyżej, można założyć, że $k < n$. Wobec tego zbiór

$\{c_0 + c_1 a + \ldots + c_{n-1} a^{n-1}, \; c_i \in K\}$

stanowi podciało ciała L, które oczywiście zawiera ciało K oraz element a. Każde ciało zawierające K oraz a musi zawierać wszystkie elementy o postaci

$c_0 + c_1 a + \ldots + c_{n-1} a^{n-1}$

wobec tego zbiór tych elementów stanowi najmniejsze rozszerzenie ciała K zawierające element a. Rozszerzenie to, jak już wspominaliśmy, oznaczamy symbolem $K(a)$.

Przykłady

1. $Q(\sqrt{2}) = \{a + b\sqrt{2} \; ; \; a, b \in Q\}$
2. $Q(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \; ; \; a, b, c \in Q\}$
3. $Q(\varepsilon_5) = \{c_0 + c_1 \varepsilon_5 + c_2 \varepsilon_5^2 + c_3 \varepsilon_5^3 \; ; \; c_i \in Q\}$

ponieważ

$$\varepsilon_5 = \cos\frac{2\pi}{5} + i \cdot \sin\frac{2\pi}{5}$$

jest liczbą algebraiczną stopnia czwartego.

4. Jeśli a jest pierwiastkiem wielomianu

$x^5 - 2x^3 + 4x^2 - 6$

to

$Q(a) = \{c_0 + c_1 a + c_2 a^2 + c_3 a^3 + c_4 a^4 \; ; \; c_i \in Q\}$

5. Jeśli a_1, a_2 są dwoma pierwiastkami tego samego wielomianu nierozkładalnego nad ciałem K, to może się zdarzyć, że $K(a_1) \neq K(a_2)$. Na przykład pierwiastkami wielomianu $x^4 - 2$ nierozkładalnego nad ciałem Q są liczby:

$$a_1 = \sqrt[4]{2}, \quad a_2 = i\sqrt[4]{2}, \quad a_3 = -\sqrt[4]{2}, \quad a_4 = -i \cdot \sqrt[4]{2}$$

Oczywiście $Q(\sqrt[4]{2}) \neq Q(i\sqrt[4]{2})$, bo pierwsze z tych ciał nie zawiera liczb nierzeczywistych, drugie zawiera liczbę nierzeczywistą $i \cdot \sqrt[4]{2}$.

6. Przykład 5 wskazuje, że na ogół ciało $K(a_1)$, gdzie a_1 jest jednym z pierwiastków wielomianu nierozkładalnego f, nie zawiera wszystkich pierwiastków tego wielomianu. Czasem jednak może być inaczej, np. $Q(\varepsilon_5)$ zawiera wszystkie pierwiastki wielomianu

$x^4 + x^3 + x^2 + x + 1$

gdyż pierwiastkami tymi są: ε_5, ε_5^2, ε_5^3, ε_5^4.

13. BAZA I STOPIEŃ ROZSZERZENIA

Stwierdziliśmy poprzednio, że jeśli a jest elementem algebraicznym stopnia n względem ciała K, to każdy element ciała $K(a)$ można zapisać w postaci

$$c_0+c_1 a+c_2 a^2+ \ldots +c_{n-1} a^{n-1}$$

Pokażemy, że zapis taki jest jednoznaczny, tj. jeśli

$$c_0+c_1 a+c_2 a^2+ \ldots +c_{n-1} a^{n-1} = d_0+d_1 a+d_2 a^2+ \ldots$$
$$\ldots +d_{n-1} a^{n-1} \qquad (1)$$

to

$$c_0 = d_0\,,\ c_1 = d_1\,,\ \ldots,\ c_{n-1} = d_{n-1} \qquad (2)$$

Gdyby bowiem miała miejsce równość (1), natomiast nie wszystkie równości (2) były spełnione, to byłoby

$$(c_0-d_0)+(c_1-d_1)\,a+(c_2-d_2)\,a^2+ \ldots +(c_{n-1}-d_{n-1})\,a^{n-1} = 0\,.$$

tj. a byłoby pierwiastkiem wielomianu

$$(c_0-d_0)+(a_1-d_1)\,x+(c_2-d_2)\,x^2+ \ldots +(c_{n-1}-d_{n-1})\,x^{n-1}$$

który nie jest zerowy (nie wszystkie współczynniki są zerami) i ma stopień mniejszy niż n (mniejszy niż stopień wielomianu minimalnego). Nie jest to możliwe, zatem przypuszczenie, że równości (2) mogą nie być spełnione, doprowadziło do sprzeczności.

Zatem elementy $1, a, a^2, \ldots, a^{n-1}$ mają następującą własność: każdy element ciała $K(a)$ ma postać

$$c_0\cdot 1+c_1\cdot a+c_2\cdot a^2+ \ldots +c_{n-1}\cdot a^{n-1}$$

(mówimy, że jest kombinacją liniową elementów $1, a, a^2, \ldots, a^{n-1}$ o współczynnikach $c_0, c_1, c_2, \ldots, c_{n-1}$ z ciała K) oraz zapis w postaci takiej kombinacji liniowej jest jednoznaczny.

Taki układ elementów zasługuje na szczególną uwagę. Niech L będzie ustalonym rozszerzeniem ciała K. Układ elementów $a_1, a_2, \ldots, a_n$ ciała L nazywamy bazą ciała L względem ciała K (albo bazą rozszerzenia $K \subset L$), gdy każdy element ciała L jest kombinacją liniową mającą postać

$$c_1 a_1+c_2 a_2+ \ldots +c_n a_n$$

o współczynnikach c_i należących do K oraz przedstawienie dowolnego elementu ciała L w postaci takiej kombinacji jest jednoznaczne.

Stwierdziliśmy wyżej, że bazą rozszerzenia $K \subset K(a)$, gdy a jest elementem algebraicznym stopnia n względem ciała K, jest układ

$$1, a, a^2, \ldots, a^{n-1}$$

Nie jest to jedyna baza, np. dla rozszerzenia $Q \subset Q(\sqrt{2})$, oprócz bazy $1, \sqrt{2}$, można jako bazę przyjąć np. układ

$$\frac{1+\sqrt{2}}{2}\,,\quad \frac{1-\sqrt{2}}{2}$$

Istotnie

$$a+b\sqrt{2} = (a+b)\cdot\frac{1+\sqrt{2}}{2}+(a-b)\cdot\frac{1-\sqrt{2}}{2}$$

więc każdy element ciała $Q(\sqrt{2})$ jest kombinacją liniową elementów

$$\frac{1+\sqrt{2}}{2}\,,\quad \frac{1-\sqrt{2}}{2}$$

Gdyby przy tym było

$$a\cdot\frac{1+\sqrt{2}}{2}+b\cdot\frac{1-\sqrt{2}}{2} = c\cdot\frac{1+\sqrt{2}}{2}+d\cdot\frac{1-\sqrt{2}}{2}$$

to

$$\frac{a+b}{2}+\frac{a-b}{2}\sqrt{2} = \frac{c+d}{2}\ \frac{c-d}{2}\sqrt{2}$$

więc

$$\frac{a+b}{2} = \frac{c+d}{2}\,,\quad \frac{a-b}{2} = \frac{c-d}{2}$$

(ponieważ zapis w postaci kombinacji liniowej elementów $1, \sqrt{2}$ jest jednoznaczny). Skąd wynika, że $a = c$ i $b = d$, Zatem możemy wyciągnąć wniosek, że dane rozszerzenie ciał może mieć wiele baz. Nasuwają się w tym miejscu następujące pytania: czy dla każdego rozszerzenia ciał istnieje baza, czy różne bazy tego samego rozszerzenia muszą mieć tyle samo elementów? Te i podobne problemy rozwiązuje algebra liniowa, tj. dział algebry zajmujący się tzw. przestrzeniami liniowymi [4].

Tu ograniczymy się do sformułowania odpowiedzi na postawione wyżej pytania. Musimy jednak nieco uogólnić wprowadzone wcześniej pojęcia bazy. Chodzi o to, że nie zawsze baza może składać się ze skończonej liczby elementów.

baza rozszerzenia

Bazą rozszerzenia $K \subset L$ nazywamy układ B elementów ciała L, gdy:

1) każdy element ciała L można przedstawić w postaci kombinacji liniowej skończonej liczby elementów zbioru B o współczynnikach z ciała K;

2) przedstawienie dowolnego elementu ciała L w postaci takiej kombinacji liniowej jest jednoznaczne, tj. w dwóch zapisach tego elementu występują te same elementy bazy, a współczynniki przy każdym z elementów bazy są w obu zapisach równe.

Ważne własności tak określonej bazy podaje następujące twierdzenie.

Twierdzenie. *Dla każdego rozszerzenia $K \subset L$ istnieje baza. Każde dwie bazy tego samego rozszerzenia są równoliczne* (tj. albo obie mają nieskończenie wiele elementów, albo obie mają po tyle samo elementów).

Przykłady

1. Każda baza rozszerzenia $Q \subset Q(\sqrt{2})$ ma dwa elementy.
2. Każda baza rozszerzenia $Q \subset Q(\sqrt[3]{2})$ ma trzy elementy.

stopień rozszerzenia

Jeśli pewna baza rozszerzenia $K \subset L$ ma n elementów (wówczas każda baza tego rozszerzenia ma n elementów), to mówimy, że stopień tego rozszerzenia wynosi n i piszemy $(L:K) = n$, jeśli natomiast pewna (a więc i każda) baza rozszerzenia $K \subset L$ ma nieskończenie wiele elementów, to mówimy, że stopień rozszerzenia $K \subset L$ jest nieskończony i piszemy $(L:K) = \infty$. Mówimy, że rozszerzenie $K \subset L$ jest skończone albo nieskończone w zależności od tego, czy stopień tego rozszerzenia jest skończony czy nieskończony.

Przy badaniu rozszerzeń skończonych interesujące i użyteczne jest następujące twierdzenie.

Twierdzenie. *Jeśli $K \subset L \subset M$ oraz $(L:K) = n$, $(M:L) = m$, to $(M:K) = mn$.*

Dowód. Niech $a_1, a_2, \ldots, a_n$ będzie bazą rozszerzenia $K \subset L$ i niech $b_1, b_2, \ldots, b_m$ będzie bazą rozszerzenia $L \subset M$. Wykażemy, że zbiór iloczynów $a_i \cdot b_j (i = 1, 2, \ldots, n, j = 1, 2, \ldots, m)$ stanowi bazę rozszerzenia $K \subset M$, a stąd wynika już teza.

Każdy element x ciała M da się zapisać w postaci kombinacji

$$x = \sum_{j=1}^{m} c_j b_j$$

której współczynniki c_j należą do ciała L. Każdy ze współczynników c_j można zapisać w postaci

$$c_j = \sum_{i=1}^{n} d_{ij} a_i$$

o współczynnikach z ciała K. Wobec tego

$$x = \sum_{j=1}^{m} \sum_{i=1}^{n} d_{ij} a_i b_j$$

tj. x jest kombinacją elementów $a_i\ b_j$ o współczynnikach d_{ij} z ciała K.

Gdyby

$$\sum_{j=1}^{m} \Big(\sum_{i=1}^{n} d_{ij} a_i \Big) b_j = \sum_{j=1}^{m} \Big(\sum_{i=1}^{n} d_{ij} a_i \Big) b_j$$

to z tego, że elementy b_j stanowią bazę, wynika

$$\sum_{i=1}^{n} d_{ij} a_i = \sum_{i=1}^{n} d'_{ij} a_i \quad \text{dla} \quad j = 1, 2, \ldots, m$$

z tego zaś, że a_i stanowią bazę, wynika

$$d_{ij} = d'_{ij} \quad \text{dla} \quad j = 1, 2, \ldots, m, \quad i = 1, 2, \ldots, n.$$

Zatem przedstawienie w postaci kombinacji liniowej elementów $a_i \cdot b_j$ jest jednoznaczne, co kończy dowód. ■

Wniosek *Jeśli $K \subset L \subset M$, to rozszerzenie $K \subset M$ jest skończone wtedy i tylko wtedy, gdy oba rozszerzenia $K \subset L$ i $L \subset M$ są skończone.*

Dowód. Jeśli $K \subset L$ i $L \subset M$ są skończone, to z powyższego twierdzenia wynika, że $(M:K) = (L:K) \cdot (M:L)$, więc $(M:K)$ jest liczbą skończoną. Jeśli zaś choć jedna z liczb $(L:K)$, $(M:L)$ jest nieskończona, to powtarzając dowód poprzedniego twierdzenia stwierdzimy, że $(M:K)$ jest nieskończony. ■

Przykłady

1. $(R:Q) = \infty$. Jeśli bowiem stopień ten byłby liczbą skończoną n, to dla każdego ciała K spełniającego zależność $Q \subset K \subset R$ byłoby $(K:Q) \cdot (R:K) = n$, skąd w szczególności wynika $(K:Q) \leqslant n$ (*). Tymczasem, jak stwierdziliśmy poprzednio, $a = \sqrt[n+1]{2}$ jest liczbą algebraiczną stopnia $n+1$, bazą rozszerzenia $Q \subset Q(a)$ jest $1, a, a^2, \ldots, a^n$, więc $(Q(a):Q) = n+1$, tj. ciało $Q(a)$ nie spełniałoby zależności (*). W rzeczywistości można udowodnić, że rozszerzenie $Q \subset R$ nie ma nawet bazy przeliczalnej.

2. $(Q(\sqrt{2}, \sqrt{3}):Q) =$

$= (Q(\sqrt{2}):Q) \cdot (Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2})) = 4,$

gdyż każdy ze stopni $(Q(\sqrt{2}):Q)$ i $(Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2}))$ wynosi dwa.

Zadania

13.1 Określić stopnie następujących rozszerzeń:

$Q \subset Q(\sqrt{2}, \varepsilon)$, gdzie

$$\varepsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$$

$Q \subset Q(\varepsilon, i)$,

$Q(\sqrt{2}) \subset Q(\sqrt[6]{2})$

13.2 Wskazać kilka baz rozszerzeń;

$Q \subset Q(\sqrt[3]{2})$, $Q \subset Q(\sqrt{2}, i)$

13.3 Przedstawić w postaci kombinacji elementów bazy

$1, \sqrt[3]{2}, \sqrt[3]{4}$ następujące elementy:

$$\frac{1}{\sqrt[3]{2}+1}, \quad \frac{1+\sqrt[3]{2}+2\sqrt[3]{4}}{2-\sqrt[3]{2}+3\sqrt[3]{4}}$$

13.4 Wykazać, że nie istnieją liczby wymierne a, b spełniające równość

$$a + b\sqrt[3]{2} = \sqrt[3]{4}$$

3. $(Q(\sqrt{2}, \sqrt[4]{2}):Q) =$

$= (Q(\sqrt{2}):Q)\cdot(Q(\sqrt{2}, \sqrt[4]{2}):Q(\sqrt{2})) = 4,$

gdyż oczywiście $(Q(\sqrt{2}):Q) = 2$ oraz

$(Q(\sqrt{2}, \sqrt[4]{2}):Q(\sqrt{2})) = \sqrt{2},$

bo $\sqrt[4]{2}$ jest pierwiastkiem wielomianu x^4-2 nierozkładalnego nad Q, ale rozkładalnego nad $Q(\sqrt{2})$ na iloczyn $(x^2-\sqrt{2})(x^2+\sqrt{2})$. Przykład ten pokazuje, że kolejne dołączanie elementów algebraicznych względem K prowadzi do rozszerzenia ciała K, którego stopień może być mniejszy od iloczynu stopni tych elementów.

4. Oczywiście $Q \subset Q(\sqrt{2}+\sqrt{3}) \subset Q(\sqrt{2}, \sqrt{3})$, więc

$(Q(\sqrt{2}+\sqrt{3}):Q)\cdot(Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2}+\sqrt{3})) =$

$= (Q(\sqrt{2}, \sqrt{3}):Q).$

Stwierdziliśmy poprzednio, że $(Q(\sqrt{2}+\sqrt{3}):Q) = 4$, (bo $\sqrt{2}+\sqrt{3}$ jest liczbą o stopniu cztery, $(Q(\sqrt{2}, \sqrt{3}):Q) = 4$, skąd wynika, że $(Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2}+\sqrt{3})) = 1$, tj. $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$.

Ponieważ rozszerzenie konstruowalne L danego ciała K powstaje w wyniku kolejnych rozszerzeń, z których każde ma stopień drugi (dołączamy pierwiastek kwadratowy), więc stopień rozszerzenia $K \subset L$ jest potęgą dwójki

$$(L:K) = 2^n$$

Każdy element $a \in L$ jest algebraiczny względem ciała K, jego stopień równy stopniowi $(K(a):K)$ jest dzielnikiem liczby 2^n, gdyż $K \subset K(a) \subset L$. Wynika stąd, że stopień elementu algebraicznego a względem ciała K jest też pewną potęgą dwójki.

Wniosek. Jeśli punkt P jest konstruowalny z danego zbioru X_0, to jego współrzędne są elementami algebraicznymi względem ciała $Q(X_0)$, przy czym stopnie tych elementów algebraicznych są potęgami dwójki.

Wniosek ten pozwala w wielu przypadkach stwierdzić, że dane zadanie konstrukcyjne jest nierozwiązalne. Pokażemy to na kilku prostych przykładach.