ALGEBRA LINIOWA 2

dr Joanna Jureczko

Politechnika Wrocławska
Wydział Elektroniki
Katedra Telekomunikacji i Teleinformatyki

Niniejsza prezentacja stanowi jedynie skrypt do wykładu. Wykład będzie wzbogacony o dodatkowe informacje, tj. dowody wybranych twierdzeń przykłady, wskazówki do zadań itp. Dodatkowe informacje dotyczące programu znajdują się w Karcie Przedmiotu.

WYKŁAD 5

Ciało
Ciało $\mathbb{Z}_p$
Podciało
Rozszerzenie ciała
Ciało Galois proste i rozszerzone

CIAŁO
CIAŁO $\mathbb{Z}_p$

Ciałem K nazywamy pierścień przemienny z jedynką, w którym
1) $0 \neq 1$
2) dla każdego $a \in K \setminus \{0\}$ istnieje $b \in K$ $\;a \cdot b = 1$.

Jeśli K jest ciałem, to $U(K) = K^* = K \setminus \{0\}$.
W szczególności K nie zawiera właściwych dzielników zera,
(tzn. jeśli $ab = 0$, to $a = 0$ lub $b = 0$ dla wszelkich $a, b \in K$).

Przykłady

Ciałami są
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$,
$\mathbb{Z}_p$, gdy p jest liczbą pierwszą, (o tym za chwilę).

Ciałami nie są $\mathbb{N}, \mathbb{Z}$,
$\mathbb{Z}_n$, gdy n jest liczbą złożoną, tzn. większą od 1 i nie jest liczbą pierwszą.

Ciało $\mathbb{Z}_p$
Liczbę całkowitą p nazywamy **liczbą pierwszą**, jeżeli jest większa od 1 i jedynymi dzielnikami tej liczby są 1 i p.

Niech p będzie liczbą pierwszą i niech

$$\mathbb{Z}_p = \{0, 1, ..., p-1\}$$

Zbiór $\mathbb{Z}_p$ z działaniami $\oplus, \odot$, gdzie $a \oplus b = (a+b)_p$ oraz $a \odot b = (a \cdot b)_p$ jest ciałem.
Przyjmijmy

$$U(\mathbb{Z}_p) = \mathbb{Z}_p^* = \{1, 2, ..., p-1\}.$$

Twierdzenie 5.1. Pierścień klas reszt $\mathbb{Z}/m\mathbb{Z}$ jest ciałem wtedy i tylko wtedy, m jest liczbą pierwszą.

PODCIAŁO
ROZSZERZENIE CIAŁA

Podciało

Załóżmy, że L jest ciałem. Podzbiór $K \subset L$ nazywamy **podciałem** ciał L, jeśli dla każdego $a, b \in K$
1) $0, 1 \in K$,
2) $a - b \in K$
3) $ab^{-1} \in K$.

Oznaczenie $K < L$.

Przykłady podciał
$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}$ jest podciałem ciała $\mathbb{R}$.
$\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \colon a, b \in \mathbb{Q}\}$ jest podciałem ciała $\mathbb{R}$.

Ciała $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ to najmniejsze ciała zawierające wszystkie liczby wymierne i liczby $\sqrt{2}$ i $\sqrt{3}$ odpowiednio.

Mówimy, że ciało L jest **rozszerzeniem** ciała K, gdy $K < L$.

Rozszerzeniem ciał nazywamy parę L/K (czyt. *L mod K*) taką, że $K < L$.

Przykład. $\mathbb{Q}(\sqrt{2})$ oraz $\mathbb{Q}(\sqrt{3})$ są rozszerzeniami ciała $\mathbb{Q}$. Oczywiście $\mathbb{Q}(\sqrt{2}) \not\subseteq \mathbb{Q}(\sqrt{3})$ oraz $\mathbb{Q}(\sqrt{3}) \not\subseteq \mathbb{Q}(\sqrt{2})$.

Ciało K nazywamy **ciałem prostym**, gdy nie zawiera podciał właściwych, tzn. podciał różnych od K.

Twierdzenie 5.2. Każde ciało zawiera pewne ciało proste.

Twierdzenie 5.3. Niech L będzie rozszerzeniem ciała K. Wtedy L jest przestrzenią liniową nad K.

Stopniem rozszerzenia ciała L ciała K, oznaczamy $[L : K]$, nazywamy wymiar L jako przestrzeni liniowej nad K.

(Definicja przestrzeni liniowej i wymiaru przestrzeni - wykład 6).

Twierdzenie 5.4. Ciało L jest **skończonym rozszerzeniem**, jeśli stopień $[L : K]$ jest skończony.

Przykład
$[\mathbb{C} : \mathbb{R}] = 2$.
$[\mathbb{R} : \mathbb{Q}] = \infty$.

ELEMENTY ALGEBRAICZNE

Elementy algebraiczne

Niech K będzie ciałem. Element $a \in K$ nazywamy **elementem algebraicznym,** gdy istnieje niezerowy wielomian o współczynnikach z ciała K, którego ten element jest pierwiastkiem. Pozostałe elementy z tego ciała to **elementy przestępne**.

Przykład.
Każda liczba wymierna q oraz każda liczba niewymierna np. $\sqrt{2}, \sqrt[5]{3}$ są pierwiastakmi pewnych wielomianów o współczynnikach wymiernych. Tutaj odpowiednio $x - q, x^2 - 2, x^5 - 3$. Ale dla π oraz e nie istnieją takie wielomiany.
Liczby π oraz e jest elementem algebraicznym względem ciała $\mathbb{R}$ ale jest elementem przestępnym względem ciała Q.

Wielomian, którego pierwiastkiem jest dany element algebraiczny nie jest wyznaczony jednoznacznie np. $\sqrt{2}$ jest pierwiastkiem $x^2 - 2$ oraz $x^4 - 4$.

Wielomian nazywamy **nierozkładalnym**, gdy nie jest on iloczynem wielomianów stopnia niższego. Oczywiście współczynniki wielomianów w rozkładzie muszą należeć do ciała K.

Przykład. Wielomian $x^2 + 1$ jest rozkładalny w $\mathbb{C}$ ale nie jest rozkładalny w $\mathbb{R}$.

Każdy wielomian stopnia dodatniego o współczynnikach z ciała K jest albo nierozkładalny albo jest iloczynem wielomianów nierozkładalnych o współczynnikach z ciała K. Rozkład wielomianu na czynniki nierozkładalne jest jednoznaczny.

Dla każdego elementu algebraicznego $a \in K$ istnieje wielomian nierozkładalny. Jest on wyznaczony jednoznacznie. **Stopniem elementu** a nazywamy stopień wielomianu nierozkładalnego, którego a jest pierwiastkiem. Taki wielomian nazywamy **wielomianem minimalnym**.

Wtedy **stopień rozszerzenia** L/K jest równy stopniowi wielomianu minimalnego. Oznaczamy $[L : K]$.

Rozważmy pierścień $K[x]$ wszystkich wielomianów o współczynnikach z ciała K. Załóżmy, że istnieje wielomian $f \in K[x]$, który nie jest rozkładalny na czynniki liniowe nad ciałem K. Wtedy ciało K trzeba rozszerzyć do ciała L, w którym wielomian f będzie rozkładalny na czynniki liniowe. Ciało L będziemy nazywać **ciałem rozkładu** wielomianu f. Zależy nam przy tym na tym, aby znaleźć najmniejsze takie ciało L rozszerzające K.

Przykład. Rozważmy element $\sqrt{2}$. Wielomianem minimalnym dla niego jest $x^2 - 2$. Taki wielomian jest nierozkładalny w $\mathbb{Q}$. Wtedy rozszerzamy $\mathbb{Q}$ do ciała $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}$. Oczywiście $(x^2 - 2)(x^2 - 3)$ nie jest rozkładalny nad $\mathbb{Q}(\sqrt{2})$ oraz $x^2 - 3$ nie jest rozkładalny nad $\mathbb{Q}(\sqrt{3})$. Wtedy takim rozszerzeniem będzie $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Przykład. Rozważmy element $\sqrt[3]{2}$. Wielomianem dla niego jest $x^3 - 2$. Ale wielomian ten, jak wiadomo ma trzy pierwiastki $\sqrt[3]{2}, \xi_3\sqrt[3]{2}, \xi_3^2\sqrt[3]{2}$, gdzie dwa ostatnie są liczbami zespolonymi. Zatem nie jest rozkładalny w $\mathbb{Q}(\sqrt[3]{2})$. Szukamy teraz wielomianu minimalnego dla elementu $\xi_3\sqrt[3]{2}$ o współczynnikach z $\mathbb{Q}(\sqrt[3]{2})$. Wielomian $x^3 - 2$ jest za duży, więc podzielimy go przez $(x - \sqrt[3]{2})$ i otrzymamy $x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$. Mamy $\mathbb{Q} < \mathbb{Q}(\sqrt[3]{2}) < \mathbb{Q}(\sqrt[3]{2})(\xi_3\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \xi_3\sqrt[3]{2})$.
Czyli stopień rozszerzenia
$[\mathbb{Q}(\sqrt[3]{2}, \xi\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt[3]{2}, \xi_3\sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] =$
$3 \cdot 2 = 6$.

CIAŁO GALOIS PROSTE I ROZSZERZONE

Niech dane będzie rozszerzenie L/K. Rozważmy grupę automorfizmów ciała L/K, tzn. odwzorowań postaci $\sigma \colon L \to L$ takich, że $\sigma(x) = x$ dla $x \in K$, (takie punkty nazywamy **punktami stałymi**).
Obserwując punkty stałe wspomnianych automorfizmów badamy w istocie najmniejsze rozszerzenie ciała, w którym dany wielomian rozkłada się na czynniki liniowe (tzn. ma wszystkie pierwiastki).

Załóżmy, że L/K jest rozszerzeniem skończonym. Grupę

$$G(L/K) = \{\sigma \in Aut(L) \colon \sigma|K = id_K\}$$

nazywamy **grupą Galois rozszerzenia** L/K.

Przykład. $L = \mathbb{C}, K = \mathbb{R}$. Wtedy
$G(\mathbb{C}/\mathbb{R}) = \{identycznosc, sprzezenie\}$.

Évariste Galois (1811–1832) – francuski matematyk o dużych zasługach dla rozwoju algebry, w szczególności **zagadnienia rozwiązywalności równań wielomianowych**. Jeden z prekursorów **teorii grup** oraz nowoczesnej **teorii równań algebraicznych (teoria Galois)**. Jako pierwszy użył nazwy grupa w odniesieniu do tej struktury algebraicznej. Mimo dużych zdolności, dwukrotnie nie zdał egzaminu do Ecole Polytechnique w Paryżu. Zginął w pojedynku w wieku 20 lat, choć istnieje też podejrzenie, że został zamordowany za sympatie republikańskie, a pojedynek jedynie upozorowano (dwa razy był więziony za publiczne wystąpienia przeciw władzy króla Ludwika Filipa). W liście napisanym ostatniej nocy przed śmiercią zawarł swoje najważniejsze idee i osiągnięcia matematyczne.

Rozszerzenie skończone $K < L$ nazywamy **rozszerzeniem Galois**, gdy K jest ciałem elementów stałych względem pewnej grupy automorfizmów z ciała L.

Przykład. $\mathbb{R} < \mathbb{C}$ jest rozszerzeniem Galois.

Twierdzenie 5.5. Niech $K < L$ będzie rozszerzeniem skończonym. Następujące warunki sa równowazne
1. $K < L$ jest rozszerzeniem Galois
2. Każdy wielomian nierozkładalny nad ciałem K i mający pierwiastek w L rozkłada sie nad L na iloczyn czynników stopnia pierwszego.
3. L jest ciałem rozkładu pewnego wielomianu o współczynnikach z ciała K
4. K jest ciałem elementów stałych względem $G(L/K)$.

Konstrukcja ciał skończonych

Niech p będzie liczbą pierwszą. Z Twierdzenia 5.1 wnosimy, że $\mathbb{Z}/p\mathbb{Z}$ jest ciałem mającym p elementów. Oznaczamy je $GF(p)$ lub $CG(p)$ (tj. Galois field,ciało Galois). Ciało to nazywamy **ciałem prostym**.

Niech p będzie liczbą pierwszą, n liczbą całkowitą dodatnią i niech f będzie wielomianem stopnia n o współczynnikach z ciała $\mathbb{Z}/p\mathbb{Z}$. Zakładamy, że ten wielomian jest nierozkładalny, (tzn. nie można przedstawić go w postaci iloczynu $f = gh$, gdzie g i h są wielomianami w $(\mathbb{Z}/p\mathbb{Z})[X]$ stopnia > 0). Jeśli wielomian nie jest nierozkładalny, to nazywamy go rozkładalnym.

Elementy ciała skończonego, które skonstruujemy, są klasami reszt modulo f. Klasa reszt wielomianu $g \in (\mathbb{Z}/p\mathbb{Z})[X]$ składa się ze wszystkich wielomianów h w $(\mathbb{Z}/p\mathbb{Z})[X]$ takich, że $g - h$ jest wielokrotnością f. Tę klasę reszt oznaczamy

$$g + f(\mathbb{Z}/p\mathbb{Z})[X] = \{g + hf \colon h \in (\mathbb{Z}/p\mathbb{Z})[X]\}.$$

Powyżej zdefiniowalismy ciało mające p^m, gdzie $m \in \mathbb{N}$ to stopień wielomianu f. To ciało nazywać będziemy **rozszerzonym ciałem Galois** oznaczać będziemy $CG(p^m)$ (lub $GF(p^m)$)).

Ciało $CG(p^m)$ jest zbiorem wielomianów stopnia $(m-1)$ o współczynnikach będących elementami z ciała $CG(p)$. Ciało to ma p^m elementów.
Dodawanie w ciele $CG(p^m)$ to dodawanie wielomianów o współczynnikach w ciele $CG(p)$.
Mnożenie w ciele $CG(p^m)$ to mnożenie wielomianów o współczynnikach w ciele $CG(p)$.

Przykład. W ciele $CG(4) = CG(2^2)$ mamy dwa wielomiany stopnia pierwszego $x, x+1$.
Wielomiany stopnia 2 nad $CG(2)$ to
$x^2 = x \cdot x$,
$x^2+1 = x^2+2x+1 = (x+1)^2 = (x+1)(x+1)$
$x^2+x = x(x+1)$
x^2+x+1. Ten wielomian jest nierozkładalny nad $CG(2)$.
Zatem $CG(4)$ to reszty z dzielenia powyższych wielomianów przez wielomian x^2+x+1, czyli mamy kolejno $\{0, 1, x, x+1\}$.

Ciało Galois służy do pozycyjnego zapisu liczb w oparciu o elementy ciała podstawowego.

Przykład. $CG(4) = CG(2^2) = \{0, 1, x, x + 1\}$ ma w zapisie pozycyjnym przedstawienie $\{00, 10, 01, 11\}$.

Element pierwotny ciała Galois

Zbiór elementów ciała Galois $CG(p^m)$ można przedstawić w postaci

$$CG(p^m) = \{a_0 + a_1\alpha + ... + a_{m-1}\alpha^{m-1} \colon a_i \in \mathbb{Z}_p\}$$

gdzie α jest pierwiastkiem wielomianu $f(x)$ stopnia m nierozkadalnego nad $\mathbb{Z}_p$.

O ile dodawaniw w $CG(p^m)$ jest łatwe, mnożenie jest bardziej skomplikowane. Dla ułatwienia tego działania stosujemy element α, taki, że

$$CG(p^m) = \{0, 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^{p^m-2}\}, \text{ gdzie } \alpha^{p^m-1} = 1.$$

Taki element będziemy nazywać **elementem pierwotnym** w $CG(p^m)$. O ile ten zapis ułatwia mnożenie, gdyż sprowadza się do obliczania potęg, to komplikuje dodawanie.

Wielomian f stopnia m o współczynnikach z ciała $CG(p)$, którego pierwiastkiem jest element pierwotny będziemy nazywać **wielomianem pierwotnym**.

Przykład. Elementy 2 oraz 3 są elementami pierwotnymi ciała $CG(5)$.
Istotnie mamy odpowiednio $2, 2^2 = 4, 2^3 = 3, 2^4 = 1$,
$3, 3^2 = 4, 3^3 = 2, 3^4 = 1$.
Element x jest elementem pierwotnym $CG(4) = CG(2^2)$. Mamy kolejno $\alpha = x, \alpha^2 = x + 1, \alpha^3 = 1$.
Mamy zatem wielomian pierwotny $f(x) = x^2 + x + 1$, bo
$f(\alpha) = \alpha^2 + \alpha + 1 = (x + 1) + x + 1 = 0$.

Zatem mamy trzy reprezentacje elementów ciała rozszerzonego
- reprezentacja wielomianowa np. dla $CG(4)$ to $0, 1, x, x + 1$,
- reprezentacja pozycyjna np. dla $CG(4)$ to $00, 01, 10, 11$
- reprezentacja potęgowa np. dla $CG(4)$ to $\alpha^0, \alpha^1, \alpha^2$.