Paweł Jamer
Promotor: dr inż. Agata Pilitowska

Wielomiany minimalne

15.06.2008

Niech K będzie rozszerzeniem ciała F i niech α będzie elementem algebraicznym nad ciałem F. Najniższy stopniem wielomian unormowany p(x) taki, że $p(\alpha) = 0$ nazywamy wielomianem minimalnym elementu α. Wielomiany minimalne odgrywają znaczącą rolę w teorii ciał skończonych. Referat dotyczyć będzie przedstawienia wybranych własności takich wielomianów oraz omówienie metod ich konstrukcji.

Spis treści

Rozdział 1

Wiadomości wstępne z algebry

Poniższy rozdział zakłada, że czytelnik jest zaznajomiony z podstawowymi strukturami algebraicznymi oraz własnościami, jakie zachodzą dla działań w tych strukturach.

1.1. Wielomiany

Definicja 1.1.1:
Niech P będzie pierścieniem przemiennym z jedynką. **Wielomianem** nad P będziemy nazywali każdy ciąg nieskończony $(a_0, a_1, a_2, \ldots)$ elementów P o co najwyżej skończonej liczbie wyrazów różnych od zera. Zbiór wszystkich wielomianów nad P będziemy oznaczali symbolem $P[x]$.

Jeśli $a = (a_0, a_1, a_2, \ldots)$ i $b = (b_0, b_1, b_2, \ldots)$ są wielomianami nad P, to ich sumę oraz iloczyn definiujemy następująco:
$a + b = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$,
$a \cdot b = (c_0, c_1, c_2, \ldots)$, gdzie $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

W dalszej części tego rozdziału, o ile nie zostanie powiedziane inaczej, symbolu P będziemy używali do oznaczania pierścienia przemiennego z jedynką.

Twierdzenie 1.1.1:
$(P[x], +, \cdot)$ jest pierścieniem przemiennym z jedynką.
Dowód:
Łączność oraz przemienność dodawania wynika bezpośrednio z jego definicji oraz łączności i przemienności dodawania w pierścieniu P. Łatwo sprawdzić, że wielomian $(0, 0, 0, 0, \ldots)$ jest elementem zerowym ze względu na dodawanie, natomiast wielomian $(-a_0, -a_1, -a_2, \ldots)$ jest elementem przeciwnym do $(a_0, a_1, a_2, \ldots)$. $(P[x], +)$ jest więc grupą abelową. Przemienność mnożenia wynika bezpośrednio z jego definicji oraz przemienności mnożenia w pierścieniu P. Weźmy teraz $a = (a_0, a_1, a_2, \ldots)$, $b = (b_0, b_1, b_2, \ldots)$, $c = (c_0, c_1, c_2, \ldots)$. Łatwo sprawdzić, że zarówno l-ty wyraz iloczynu $(a \cdot b) \cdot c$, jak i l-ty wyraz iloczynu $a \cdot (b \cdot c)$ jest postaci $\sum_{i+j+k=l} a_i b_j c_k$, co dowodzi łączności mnożenia. Z oczywistej równości $\sum_{i=0}^{k} (a_i + b_i) \cdot c_{k-i} = \sum_{i=0}^{k} a_i \cdot c_{k-i} + \sum_{i=0}^{k} b_i \cdot c_{k-i}$ wynika rozdzielność mnożenia względem dodawania. $(P[x], +, \cdot)$ jest więc pierścieniem przemiennym. Łatwo sprawdzić, że jedynką tego pierścienia jest wielomian $(1, 0, 0, 0, \ldots)$. □

Definicja 1.1.2:
Niech $a = (a_0, a_1, a_2, \ldots)$ będzie wielomianem nad P. **Stopniem wielomianu** a nazywamy taką liczbę n, że $a_n \neq 0$ oraz $(\forall k > n)\, a_k = 0$. Dodatkowo stopień wielomianu zerowego definiujemy jako $-\infty$, przyjmując umowę, że $-\infty < k$ oraz $-\infty + k = -\infty$ dla dowolnego $k \in \mathbb{Z}$. Stopień wielomianu a oznaczać będziemy symbolem $\deg a$.

Twierdzenie 1.1.2:
Niech $a, b \in P[x]$, wówczas:

1. $\deg(a + b) \leq \max(\deg a, \deg b)$,
2. $\deg(a \cdot b) \leq \deg a + \deg b$,

3. jeśli P jest pierścieniem bez dzielników zera, to $\deg(a \cdot b) = \deg a + \deg b$.

Dowód:
Niech $a = (a_0, a_1, a_2, \ldots)$ i $b = (b_0, b_1, b_2, \ldots)$. Przyjmijmy bez straty ogólności, że $\deg a \geq \deg b$.

1. Mamy dla $k > \deg a$ $a_k + b_k = 0$, a więc wielomian $\deg(a+b) \leq \deg a = \max(\deg a, \deg b)$.
2. Mamy dla $k > \deg a + \deg b$: $\sum_{i=0}^{k} a_i b_{k-i} = 0$, a więc $\deg(a \cdot b) \leq \deg a + \deg b$.
3. Niech $d = \deg a + \deg b$. Zauważmy, że $(\forall i < \deg a)\, b_{d-i} = 0 \Rightarrow a_i \cdot b_{d-i} = 0$ oraz $(\forall i > \deg b)\, a_i = 0 \Rightarrow a_i \cdot b_{d-i} = 0$, a więc $\sum_{i=0}^{d} a_i \cdot b_{d-i} = a_{\deg a} \cdot b_{\deg b}$. Ponieważ $a_{\deg a} \neq 0$ oraz $b_{\deg b} \neq 0$ z definicji, a P jest pierścieniem bez dzielników zera, więc $a_{\deg a} \cdot b_{\deg b} \neq 0$. Pokazaliśmy więc, że d-ty wyraz wielomianu $a \cdot b$ jest niezerowy. Ponadto, z poprzedniego punktu wiemy, że $\deg(a \cdot b) \leq d$, a więc musi być $\deg(a \cdot b) = d$.□

Definicja 1.1.3:
Wielomian $(a_0, a_1, a_2, \ldots)$ stopnia n nad P nazywamy **unormowanym** jeśli $a_n = 1$.

Definicja 1.1.4:
Wielomian stopnia dodatniego nazywamy **rozkładalnym** w pierścieniu P jeśli można przedstawić go w postaci dwóch innych wielomianów stopnia dodatniego z $P[x]$. Jeśli wielomian nie jest rozkładalny, to mówimy, że jest **nierozkładalny** w P.

Twierdzenie 1.1.3:
Odwzorowanie $\varepsilon : P \to P[x]\,;\, a \mapsto (a, 0, 0, 0, \ldots)$ jest różnowartościowym homomorfizmem pierścieni, przeprowadzającym jedynkę pierścienia P na jedynkę pierścienia $P[x]$. Ponadto mamy $\varepsilon(a) \cdot (a_0, a_1, a_2, \ldots) = (aa_0, aa_1, aa_2, \ldots)$ dla dowolnego $a \in P$ i $(a_0, a_1, a_2, \ldots) \in P[x]$.
Dowód:
Niech $a, b \in P$. Mamy wówczas bezpośrednio z definicji dodawania $\varepsilon(a+b) = (a+b, 0, 0, 0, \ldots) = (a, 0, 0, 0, \ldots) + (b, 0, 0, 0, \ldots) = \varepsilon(a) + \varepsilon(b)$ oraz z definicji mnożenia $\varepsilon(a \cdot b) = (a \cdot b, 0, 0, 0, \ldots) = (a, 0, 0, 0, \ldots) \cdot (b, 0, 0, 0, \ldots) = \varepsilon(a) \cdot \varepsilon(b)$. Więc ε jest homomorfizmem. Zachodzi $\varepsilon(1) = (1, 0, 0, 0, \ldots)$, a więc jedynka pierścienia P jest przeprowadzana na jedynkę pierścienia $P[x]$. Niech teraz $\varepsilon(a) = \varepsilon(b)$. Wynika stąd, że $(a, 0, 0, 0, \ldots) = (b, 0, 0, 0, \ldots) \Rightarrow a = b$, a więc ε jest różnowartościowe. Podstawiając $(a, 0, 0, 0, \ldots)$ za $\varepsilon(a)$ do równości z tezy twierdzenia i mnożąc wielomiany można łatwo pokazać, że jest ona prawdziwa. □

Powyższe twierdzenie pozwala na utożsamienie każdego elementu $a \in P$ z odpowiadającym mu wielomianem $(a, 0, 0, 0, \ldots) \in P[x]$. Jeśli przyjmiemy jeszcze oznaczenie x na wielomian $(0, 1, 0, 0, 0, \ldots)$ możemy udowodnić następujące twierdzenie.

Twierdzenie 1.1.4:
Jeśli $a = (a_0, a_1, a_2, \ldots)$ i $\deg a \leq n$, to $a = a_0 + a_1 x + \ldots + a_n x^n$.
Dowód:
Przeprowadzimy dowód indukcyjny po n.
Dla $n = 0$ twierdzenie w oczywisty sposób jest prawdziwe.
Załóżmy więc, że jest ono prawdziwe dla $n-1$ i pokażmy, że jest również prawdziwe dla n. Łatwo sprawdzić, że spełniony jest następujący ciąg równości $a = (a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots) = (a_0, 0, 0, 0, \ldots) + (0, a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots) = a_0 + (a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots)\, x$.
Stosując założenie indukcyjne do ciągu $(a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots)$ dostajemy $a = a_0 + \left(a_1 + a_2 x + \ldots + a_n x^{n-1}\right) x = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$. □

Możemy więc od teraz zapisywać wielomiany w ogólnie przyjętej postaci $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$. Pamiętając jednak, że wielomian, w przeciwieństwie do tego, co mógłby sugerować symbol $p(x)$, nie jest funkcją. Każdemu wielomianowi możemy jednak przyporządkować funkcję, co też zaraz uczynimy.

Definicja 1.1.5:
Niech $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in P[x]$. Funkcję $p : P \to P; t \mapsto a_0+a_1t+a_2t^2+\ldots+a_nt^n$ nazywamy **funkcją wielomianową** nad pierścieniem P wyznaczoną przez wielomian $p(x)$.

Twierdzenie 1.1.5:
Jeśli P jest pierścieniem przemiennym z jedynką, to odwzorowanie $\Phi : P[x] \to \mathrm{Map}(P,P)$, gdzie $\mathrm{Map}(P,P)$ jest zbiorem wszystkich odwzorowań z P w P, przyporządkowujące wielomianowi $p(x)$ wyznaczoną przez ten wielomian funkcję wielomianową $p(t)$ na P, jest homomorfizmem pierścieni.
Dowód:
Sprowadza się do pokazania, że $\Phi(p(x)+q(x)) = \Phi(p(x)) + \Phi(q(x))$ oraz $\Phi(p(x)\cdot q(x)) = \Phi(p(x))\cdot\Phi(q(x))$ poprzez skorzystanie bezpośrednio z definicji funkcji Φ oraz elementarnych własności działań w pierścieniach P i $P[x]$. Proste obliczenia pozostawmy zainteresowanym czytelnikom. □

Definicja 1.1.6:
Mówimy, że $t \in P$ jest **pierwiastkiem wielomianu** $p(x) \in P[x]$ jeśli $p(t) = 0$.

Twierdzenie 1.1.6 (algorytm dzielenia dla wielomianów):
Niech F będzie ciałem i niech $f(x), g(x) \in F[x]$. Jeśli $g(x) \neq 0$, to istnieją jednoznacznie wyznaczone wielomiany $q(x), r(x) \in F[x]$ takie, że

$$f(x) = q(x)\cdot g(x) + r(x),$$

gdzie $r(x) = 0$ lub $\deg r(x) < \deg g(x)$.
Dowód:
Niech $g(x) = b_0 + b_1x + \ldots + b_mx^m$. Przeprowadzimy indukcję, ze względu na stopień wielomianu $f(x)$. Jeśli $\deg f(x) < m$, to $f(x) = 0\cdot g(x) + f(x)$. Załóżmy więc, że twierdzenie jest prawdziwe dla wielomianów stopnia mniejszego niż $n \geq m$. Niech $f(x) = a_0 + a_1x + \ldots + a_nx^n$, gdzie $a_n \neq 0$. Niech $p(x) = f(x) - b_m^{-1}a_nx^{n-m}g(x)$. Łatwo zauważyć, że $\deg p(x) < n$. Zatem na mocy założenia indukcyjnego $p(x) = h(x)g(x) + r(x)$. Stąd $f(x) = p(x) + b_m^{-1}a_nx^{n-m}g(x) = q(x)\cdot g(x) + r(x)$, gdzie $q(x) = h(x) + b_m^{-1}a_nx^{n-m}$. Pozostaje nam wykazanie jednoznaczności, przypuśćmy więc, że $q_1(x)g(x)+r_1(x) = q_2(x)g(x)+r_2(x)$, gdzie $\deg r_1(x) < \deg g(x)$ i $\deg r_2(x) < \deg g(x)$. Wtedy $r_1(x) - r_2(x) = (q_2(x) - q_1(x))g(x)$. Stąd $q_2(x) - q_1(x) = 0$, w przeciwnym bowiem razie mielibyśmy $\deg(r_1(x) - r_2(x)) \geq \deg g(x)$, mimo założenia, że $\deg r_1(x) < \deg g(x)$ i $\deg r_2(x) < \deg g(x)$. Stąd także $r_1(x) - r_2(x) = 0$. □

Twierdzenie 1.1.7:
Niech F będzie ciałem. Jeśli $f(x) \in F[x]$ i $a \in F$, to istnieje jednoznacznie wyznaczony wielomian $g(x)$ nad P taki, że

$$f(x) = (x-a)g(x) + f(a).$$

Dowód:
Z twierdzenia 1.1.6 wynika, że dla wielomianów $f(x)$ oraz $x - a$ muszą istnieć jednoznacznie wyznaczone wielomiany $g(x)$ oraz r(x) takie, że $f(x) = (x-a)g(x) + r(x)$. Ponadto $\deg r(x) < 1$ oraz $r(a) = f(a) - (a-a)g(a) = f(a)$, a więc $r(x) = f(a)$. □

Twierdzenie 1.1.8:
Niech F będzie ciałem. Jeśli $p(x) \in F[x]$ jest wielomianem stopnia n, to $f(x)$ ma co najwyżej n różnych pierwiastków w F.
Dowód:
Przeprowadźmy indukcję względem n. Oczywiste jest, że dla $n = 0$ teza jest

prawdziwa. Załóżmy więc, że twierdzenie jest prawdziwe dla $n-1$. Niech teraz $\deg p(x) = n$ i niech $x_0, x_1, \ldots, x_n$ będą pierwiastkami wielomianu $p(x)$ takimi, że $x_i \neq x_j$ dla $i \neq j$. Ponieważ $p(x_0) = 0$, to $p(x) = (x - x_0)\, g(x)$. Jako, że $p(x_i) = 0$ oraz $(x_i - x_0) \neq 0$ dla $i = 1, \ldots, n$, więc musi być $g(x_i) = 0$ dla $i = 1, \ldots n$. Jest to jednak sprzeczne z założeniem indukcyjnym. □

1.2. Rozszerzenia ciał

Definicja 1.2.1:
Podciałem ciała K nazywamy podpierścień F, który jest również ciałem. Ciało K nazywamy **rozszerzeniem ciała** F.

Twierdzenie 1.2.1:
Jeśli K jest rozszerzeniem ciała F, to K tworzy strukturę przestrzeni wektorowej nad F.
Dowód:
Polega na łatwym sprawdzeniu poprawności aksjomatów przestrzeni wektorowej. □

Definicja 1.2.2:
Wymiar przestrzeni wektorowej K nad F nazywa się stopniem **rozszerzenia ciała** K nad F i oznacza $[K : F]$.

Definicja 1.2.3:
Niech K będzie rozszerzeniem ciała F i niech $a \in K$. Najmniejsze podciało ciała K zawierające $F \cup \{a\}$ nazywamy **ciałem otrzymanym z** F **przez dołączenie elementu** a i oznaczamy symbolem $F(a)$.

Definicja 1.2.4:
Niech K będzie rozszerzeniem ciała F. Element $u \in K$ nazywamy **algebraicznym** nad F, jeśli istnieją $a_0, a_1, a_2, \ldots, a_n \in F$, nie wszystkie równe zero i takie, że $a_0 + a_1 u^1 + a_2 u^2 + \ldots + a_n u^n = 0$.

Twierdzenie 1.2.2:
Niech K rozszerzenie ciała F, $u \in K$ algebraiczny nad F, $p(x) \in F[x]$ nierozkładalny nad F stopnia n o pierwiastku u. Wtedy

$$F(u) \cong F[x] / (p(x)),$$

ponadto

$$F(u) = \left\{ \sum_{i=0}^{n-1} c_i u^i \mid c_i \in F \right\}.$$

Dowód:
Niech $f : F[x] \to F(\alpha)\,;\, g(x) \mapsto g(\alpha)$. Łatwo sprawdzić, że f jest homomorfizmem pierścieni, a więc $\mathrm{Ker} f$ jest ideałem $F[x]$. Jako, że $F[x]$ jest pierścieniem ideałów głównych, więc $\mathrm{Ker} f = (r(x))$, dla pewnego $r(x)$ takiego, że $r(u) = 0$. Wiemy, że $p(u) = 0 \Rightarrow p(x) \in (r(x))$, tzn. $r(x) \mid p(x)$, ale $p(x)$ jest nierozkładalny, więc $p(x) = kr(x)$, $k \neq 0 \Rightarrow \mathrm{Ker} f = (r(x)) = (p(x))$. Z twierdzenia o izomorfizmie dla pierścieni mamy $F[x] / (p(x)) \cong f(F[x]) \subseteq F(u)$. Jednak $f(F[x])$ zawiera F oraz u, a więc $f(F[x]) = F(u)$ i $F[x] / (p(x)) \cong F(u)$. □

Definicja 1.2.5:
Charakterystyką pierścienia R nazywamy najmniejszą liczbę całkowitą dodatnią $g > 0$ taką, że $g \cdot a = 0$, $\forall a \in R$. Jeśli taka liczba nie istnieje, to charakterystyka R jest równa zero.

Kolejne twierdzenie i wynikający z niego wniosek przyjmiemy bez dowodu.

Twierdzenie 1.2.3:

1. Niech F - ciało o charakterystyce p (p - liczba pierwsza), wówczas F zawiera podciało izomorficzne z $\mathbb{Z}_p$.
2. Niech F - ciało o charakterystyce 0, wówczas F zawiera podciało izomorficzne z $\mathbb{Q}$.

Wniosek 1.2.1:
Charakterystyka ciała skończonego jest niezerowa.

1.3. Ciała Galois

Definicja 1.3.1:
Ciało skończone zawierające p^m elementów nazywamy **ciałem Galois** rzędu p^m i oznaczamy symbolem $GF(p^m)$.

Twierdzenie 1.3.1:
Każde ciało skończone zawiera p^m elementów, gdzie p liczba pierwsza, m dodatnia liczba całkowita.
Dowód:
Niech F będzie ciałem skończonym. Jako takie, ma ono charakterystykę p będącą liczbą pierwszą, a więc zawiera podciało izomorficzne z $\mathbb{Z}_p$, jest ono więc rozszerzeniem $\mathbb{Z}_p$. Niech $[F:\mathbb{Z}_p] = m$, wówczas istnieje $\{f_1, f_2, \ldots, f_m\}$ baza przestrzeni wektorowej F nad $\mathbb{Z}_p$, a więc $F = \{\sum_{i=1}^{m} \lambda_i f_i \mid \lambda_i \in \mathbb{Z}_p\}$. Każda λ_i może przyjąć p różnych wartości więc $|F| = p^m$. □

Twierdzenie 1.3.2:
Każdy niezerowy element ciała Galois jest algebraiczny.
Dowód:
Niech $v \in GF(p^m)$ i $v \neq 0$. Wiemy, że $GF(p^m) = \left\{\sum_{i=0}^{m-1} c_i u^i \mid c_i \in \mathbb{Z}_p\right\}$, w takim razie $v = a_0 + a_1 u + a_2 u^2 + \ldots + a_{m-1}u^{m-1}$, gdzie $a_i \in \mathbb{Z}_p$. Gdyby zachodziło $a_i = 0$ dla każdego $i = 1, \ldots, m$, to $v = 0+0u+0u^2+\ldots+0u^{m-1} = 0$. Zakładaliśmy jednak, że $v \neq 0$, musi więc istnieć takie i dla którego zachodzi $a_i \neq 0$. Tym samym v jest algebraiczny. □

Kolejne twierdzenie przyjmiemy bez dowodu.

Twierdzenie 1.3.3:
Niech $GF(p^m)^* = GF(p^m) - \{0\}$. $GF(p^m)^*$ z mnożeniem jest grupą cykliczną.

Definicja 1.3.2:
Generator grupy cyklicznej $GF(p^m)^*$ nazywamy **elementem pierwotnym** ciała $GF(p^m)$.

Definicja 1.3.3:
Rzędem niezerowego elementu $u \in GF(q)$ nazywamy najmniejsze $r \in \mathbb{N}$ takie, że $u^r = 1$ i oznaczamy przez rzu.

Twierdzenie 1.3.4:
Rząd dowolnego niezerowego elementu ciała $GF(q)$ jest dzielnikiem $q-1$.
Dowód:
Zauważmy najpierw, że rząd elementu pierwotnego u ciała $GF(q)$ to $q-1$. Niech teraz v będzie dowolnym niezerowym element ciała $GF(q)$ o rzędzie $r \in \mathbb{N}$, a więc $v^r = 1$. Element v można przedstawić jako u^s dla pewnego $s \in \{1, \ldots, q-1\}$. Więc $(u^s)^r = u^{sr} = 1$, ale $u^t = 1 \Leftrightarrow t = k(q-1)$. Musi więc zachodzić równość $sr = k(q-1) \Rightarrow s = \frac{k(q-1)}{r} \in \{1, \ldots, q-1\}$, a to w szczególności implikuje, że r jest dzielnikiem $q-1$. □

Twierdzenie 1.3.5:
Każdy element ciała $GF(q)$ spełnia równanie

$$x^{q^n} - x = 0$$

dla dowolnego $n \in \mathbb{N}$.
Dowód:
Pokażemy prawdziwość twierdzenia przez indukcję względem n. Dla $n = 0$ twierdzenie jest oczywiście prawdziwe. Pokażmy prawdziwość twierdzenia dla $n = 1$. Jako, że rząd dowolnego niezerowego elementu ciała $GF(q)$ jest dzielnikiem $q-1$, więc każdy element tego ciała spełnia równanie $x^{q-1} - x = 0$. Oczywiście $x = 0$ również spełnia to równanie, a więc spełnia je każdy element ciała. W takim razie każdy element ciała spełnia również równanie $x\left(x^{q-1} - x\right) = 0 \Leftrightarrow x^q - x = 0$. Załóżmy teraz, że twierdzenie jest prawdziwe dla pewnego $n-1$. Wobec podstawy oraz założenia indukcyjnego mamy wówczas $x^{q^n} = \left(x^{q^{n-1}}\right)^q = x^q = x$ $\Rightarrow x^{q^n} - x = 0$. $\square$

Twierdzenie 1.3.6:
Dla dowolnego wielomianu $p(x)$ nad ciałem $GF(p)$, gdzie p jest liczbą pierwszą oraz dowolnej liczby $n \in \mathbb{N}$ zachodzi

$$[p(x)]^{p^n} = p\left(x^{p^n}\right).$$

Dowód:
Pokażmy najpierw, że dla dowolnych wielomianów Q, R nad ciałem charakterystyki p oraz dla dowolnego $n \in \mathbb{N}$ zachodzi

$$(Q+R)^{p^n} = Q^{p^n} + R^{p^n}.$$

Pokażmy, że równość zachodzi dla $n = 1$. Korzystając ze wzoru dwumianowego dostajemy

$$(Q+R)^p = \sum_{i=0}^{r} \left(\begin{array}{c} p \\ i \end{array} \right) Q^i R^{p-i},$$

gdzie iloczyn $\left(\begin{array}{c} p \\ i \end{array} \right) Q^i R^{p-i}$ rozumiemy jako sumę $\left(\begin{array}{c} p \\ i \end{array} \right)$ wyrazów postaci $Q^i R^{p-i}$. Zauważmy, że

$$\left(\begin{array}{c} p \\ i \end{array} \right) = \frac{(p-i+1)\cdot(p-i+2)\cdot\ldots\cdot p}{1\cdot 2\cdot\ldots\cdot i}$$

dla $1 < i < p$ jest wielokrotnością p. Więc dla $1 < i < p$ suma $\left(\begin{array}{c} p \\ i \end{array} \right)$ identycznych składników w ciele charakterystyki p jest równa zero. Załóżmy, że równość jest prawdziwa dla wszystkich $k < n$. Dla n mamy wtedy

$$\begin{aligned} (Q+R)^{p^n} &= \left((Q+R)^{p^{n-1}}\right)^p \\ &= \left(Q^{p^{n-1}} + R^{p^{n-1}}\right)^p \\ &= \left(Q^{p^{n-1}}\right)^p + \left(R^{p^{n-1}}\right)^p \\ &= Q^{p^n} + R^{p^n}. \end{aligned}$$

Pokazaliśmy tym samym, że $(Q+R)^{p^n} = Q^{p^n} + R^{p^n}$ zachodzi. Łatwo zauważyć teraz, że zachodzi również

$$\begin{aligned} (Q_1 + Q_2 + \ldots + Q_n)^{p^n} &= Q_1^{p^n} + (Q_2 + \ldots + Q_n)^{p^n} \\ &= \ldots \\ &= Q_1^{p^n} + Q_2^{p^n} + \ldots + Q_n^{p^n}. \end{aligned}$$

Kożystając z tak otrzymanej równości oraz twierdzenia 1.3.5 można ostatecznie pokazać, że

$$\begin{aligned}
[p(x)]^{p^n} &= \left(\sum_{i=0}^{r} a_i x^i\right)^{p^n} \\
&= \sum_{i=0}^{r} \left(a_i x^i\right)^{p^n} \\
&= \sum_{i=0}^{r} a_i^{p^n} x^{i \cdot p^n} \\
&= \sum_{i=0}^{r} a_i \left(x^{p^n}\right)^i \\
&= p\left(x^{p^n}\right).
\end{aligned}$$

□

Pomijając w dowodzie powyższego twierdzenia dwie ostatnie równości dostajemy dowód poniższego twierdzenia.

Twierdzenie 1.3.7:
Dla dowolnego wielomianu

$$p(x) = \sum_{i=0}^{r} a_i x^i$$

nad ciałem $GF(p^m)$ i dowolnego $n \in \mathbb{N}$ zachodzi

$$[p(x)]^{p^n} = \sum_{i=0}^{r} a_i^{p^n} x^{ip^n}.$$

Warto zauważyć, że przy takim sformułowaniu twierdzenia, nie jest możliwe zastosowanie do niego twierdzenia 1.3.5, a więc nie możemy przyjąć, że $a_i^{p^n} = a_i$.

Rozdział 2

Wielomiany minimalne

2.1. Definicja i jednoznaczność

Definicja 2.1.1:
Niech K będzie rozszerzeniem ciała F, a $u \in K$ elementem algebraicznym nad F. Najniższy stopniem wielomian unormowany $p(x)$ taki, że u jest jego pierwiastkiem nazywamy **wielomianem minimalnym** elementu u.

Twierdzenie 1.3.1 (o jednoznaczności wielomianu minimalnego):
Niech K będzie rozszerzeniem ciała F, a $u \in K$ elementem algebraicznym nad F. Istnieje wtedy jednoznacznie wyznaczony wielomian będący wielomianem minimalnym elementu u.
Dowód:

1. Istnienie.
   Niech S będzie zbiorem wszystkich niezerowych wielomianów nad F o pierwiastku u. Skoro u jest elementem algebraicznym nad F, więc $S \neq \emptyset$. Stopnie wielomianów należących do zbioru S tworzą zbiór niepusty liczb całkowitych dodatnich, więc na mocy aksjomatu dobrego porządku zbiór ten musi zawierać element najmniejszy. Weźmy $m(x) \in S$ o najmniejszym stopniu. Pomnożenie $m(x)$ przez dowolną, niezerową stałą daje wielomian tego samego stopnia o pierwiastku u. Możemy więc przyjąć, że $m(x)$ jest unormowany. Tym samym $m(x)$ jest wielomianem minimalnym elementu u.
2. Jednoznaczność
   Niech $m(x)$ będzie wielomianem minimalnym elementu u. Załóżmy, że istnieje różny od $m(x)$ wielomian minimalny $p(x)$ elementu u. Niech $t(x) = m(x) - p(x)$. Z unormowania wielomianów $m(x)$, $p(x)$ wynika, że mają one ten sam współczynnik przy najwyższej potędze, a więc wielomian $t(x)$, będący ich różnicą, przy tejże potędze będzie miał współczynnik zero, w takim razie $\deg t(x) < \deg m(x) = \deg p(x)$. Z definicji wielomianu minimalnego dostajemy $t(u) = m(u) - p(u) = 0 - 0 = 0$. Podobnie jak w dowodzie istnienia możemy przyjąć, że $t(x)$ jest unormowany. Tym samym znaleźliśmy wielomian unormowany o pierwiastku u niższego stopnia od wielomianu minimalnego $m(x)$. Jednak $m(x)$ jest wielomianem najniższego stopnia spełniającym te własności. Otrzymana sprzeczność dowodzi, że istnieje dokładnie jeden wielomian minimalny. □

Wniosek 2.1.1:
Niech K będzie rozszerzeniem ciała F, a $u \in K$ elementem algebraicznym nad F. Jeśli $m(x) \in F[x]$ jest wielomianem minimalnym elementu u, to jest on wielomianem najniższego stopnia o pierwiastku u.
Dowód:
Gdyby istniał wielomian niższego stopnia o pierwiastku u moglibyśmy go unormować, uzyskując wielomian minimalny różny od $m(x)$, co z jednoznaczności wielomianu minimalnego jest niemożliwe. □

Przykład 2.1.1:

1. Weźmy wielomian unormowany $m(x) = x^2 + 1 \in \mathbb{R}[x]$ oraz $i \in \mathbb{C}$. Mamy wówczas $m(i) = i^2 + 1 = -1 + 1 = 0$. Co więcej wielomian $m(x)$ jest

najniższego stopnia wielomianem o pierwiastku i nad ciałem $\mathbb{R}$. Więc x^2+1 jest wielomianem minimalnym elementu algebraicznego $i \in \mathbb{C}$ nad ciałem $\mathbb{R}$.

2. Niech $m(x) = x^2 - 3 \in \mathbb{Q}[x]$. Dla $\sqrt{3} \in \mathbb{R}$ mamy $m\left(\sqrt{3}\right) = \left(\sqrt{3}\right)^2 - 3 = 3-3 = 0$. Ponadto wielomian x^2-3 nad $\mathbb{Q}$ jest wielomianem unormowanym najmniejszego stopnia o pierwiastku $\sqrt{3}$. Jest więc wielomianem minimalnym elementu $\sqrt{3}$. Gdybyśmy jednak rozważali $m(x) = x^2-3 \in \mathbb{R}[x]$ moglibyśmy rozłożyć wielomian ten na $m(x) = \left(x-\sqrt{3}\right)\left(x+\sqrt{3}\right)$. Wówczas wielomianem minimalnym elementu $\sqrt{3}$ byłby wielomian $x-\sqrt{3}$.
3. Weźmy $u = \sqrt{3}+\sqrt{5} \in \mathbb{R}$. Wówczas $u^2 = 3+2\sqrt{3}\sqrt{5}+5 = 8+2\sqrt{15}$ $\Rightarrow u^2 - 8 = 2\sqrt{15} \Rightarrow \left(u^2-8\right)^2 = 60 \Rightarrow \left(u^2-8\right)^2 - 60 = 0$. Niech więc $m(x) = \left(x^2-8\right)^2-60 = x^4-16x^2+4 \in \mathbb{Q}[x]$. Można wykazać, że wielomian $m(x)$ jest wielomianem unormowanym najniższego stopnia o pierwiastku $\sqrt{3}+\sqrt{5}$ nad $\mathbb{Q}$, a więc jest wielomianem minimalnym.

2.2. Własności

Twierdzenie 2.2.1:
Niech K będzie rozszerzeniem ciała F, $u \in K$ elementem algebraicznym nad F, $m(x) \in F[x]$ wielomianem minimalnym elementu u, wówczas

$$(\forall g(x) \in F[x])\, g(u) = 0 \Rightarrow m(x) \mid g(x).$$

Dowód:
Niech $g(x) \in F[x]$, $g(u) = 0$. Z algorytmu dzielenia dla wielomianów wiemy, że

$$(\exists! q(x), r(x) \in F[x])\, g(x) = q(x)m(x) + r(x),$$

gdzie $r(x) = 0$ lub $\deg r(x) < \deg m(x)$. Załóżmy, że $r(x) \neq 0$. Przekształcając powyższą równość dostajemy $r(u) = g(u) - q(u)p(u) = 0 - q(u)0 = 0$. Z twierdzenia o stopniu wielomianu minimalnego i z nierówności $\deg r(x) < \deg m(x)$ wynika, że jest to niemożliwe. Więc musi zachodzić $r(x) = 0$, a stąd dostajemy $m(x) \mid g(x)$. □

Twierdzenie 2.2.2:
Niech K będzie rozszerzeniem ciała F, a $u \in K$ elementem algebraicznym nad F. Warunek minimalności stopnia wielomianu minimalnego $m(x) \in F[x]$ elementu u jest równoważny nierozkładalności $m(x)$ w F.
Dowód:
Gdyby $m(x)$ był rozkładalny to

$$(\exists p(x), q(x) \in F[x])\, m(x) = p(x)q(x),$$

$\deg p(x) < \deg m(x)$ i $\deg q(x) < \deg m(x)$. Wówczas

$$m(u) = p(u)q(u) \Rightarrow p(u) = 0 \vee q(u) = 0,$$

zgodnie z wnioskiem 2.1.1 jest to jednak niemożliwe. Niech teraz wielomian nierozkładalny $p(x)$ spełnia wszystkie aksjomaty wielomianu minimalnego elementu u poza minimalnością stopnia. W takim razie istnieje inny wielomian $q(x)$ będący wielomianem minimalnym elementu u. Z poprzedniego twierdzenia wynika więc, że

$$q(x) \mid p(x) \Leftrightarrow (\exists r(x) \in F[x])\, p(x) = r(x)\, q(x),$$

ale wielomian $p(x)$ jest nierozkładalny. Otrzymana sprzeczność dowodzi więc, że $p(x)$ musi być wielomianem minimalnym.□

Twierdzenie 2.2.3:
Jeśli $m(x) \in GF(p)[x]$ jest wielomianem minimalnym elementu $u \in GF(p^m)$, to $\deg m(x) \leq m$.
Dowód:
Niech $m(x) \in GF(p)[x]$ będzie wielomianem minimalnym elementu $u \in GF(p^m)$. $GF(p^m)$ tworzy nad $\mathbb{Z}_p$ przestrzeń wektorową taką, że $\dim GF(p^m) = m$. Zauważamy, że układ wektorów 1, u, u^2, $\ldots$, u^m musi być w tej sytuacji liniowo zależny. Tym samym

$$(\exists a_i \in \mathbb{Z}_p, \text{ nie wszystkie równe } 0) \sum_{i=0}^{m} a_i u^i = 0.$$

Możemy więc zdefiniować

$$p(x) = \sum_{i=0}^{m} a_i x^i \ (\deg p(x) \leq m)$$

o pierwiastku u. Z twierdzenia o podzielnikach wielomianu minimalnego

$$m(x) \mid p(x) \Rightarrow p(x) = q(x)\, m(x),$$

a więc

$$m \geq \deg p(x) = \deg(q(x)\, m(x)) = \deg q(x) + \deg m(x)$$

$\Rightarrow \deg m(x) \leq m - \deg q(x) \leq m$.□

Twierdzenie 2.2.4:
Jeśli $m(x) \in GF(p)[x]$ jest wielomianem minimalnym elementu pierwotnego ciała $GF(p^m)$, to $\deg m(x) = m$.
Dowód:
Niech $m(x) \in GF(p)[x]$ będzie wielomianem minimalnym elementu pierwotnego $u \in GF(p^m)$, $\deg m(x) = d$. Z twierdzenia o postaci ciała otrzymanego przez dołączenie elementu dostajemy

$$GF\left(p^d\right) = \mathbb{Z}_p(u) = \left\{ \sum_{i=0}^{d-1} c_i u^i \mid c_i \in \mathbb{Z}_p \right\}.$$

Stąd dostajemy, że $GF\left(p^d\right) \ni u$ element pierwotny $GF(p^m)$, a zatem

$$GF(p^m) \subseteq GF\left(p^d\right) \Rightarrow m \leq d.$$

Z drugiej strony, poprzednie twierdzenie daje nam $d \leq m$, więc ostatecznie $d = m$. □

Definicja 2.2.1:
Wielomianem pierwotnym nazywamy wielomian minimalny elementu pierwotnego ciała.

Twierdzenie 2.2.5:
Elementy $u, u^p \in GF(p^m)$ mają ten sam wielomian minimalny $m(x) \in GF(p)[x]$.
Dowód:
Niech $m_1(x) \in GF(p)[x]$ będzie wielomianem minimalnym elementu $u \in GF(p^m)$, natomiast $m_2(x) \in GF(p)[x]$ wielomianem minimalnym elementu u^p. Z twierdzenia 1.3.6 dostajemy

$$m_1(u^p) = [m_1(u)]^p = 0,$$

a zatem (z twierdzenia 2.2.1) mamy $m_2(x) \mid m_1(x)$. Pamiętając, że w w ciele $GF(p^m)$ każdy element spełnia równanie $x^{p^m} = x$ (twierdzenie 1.3.5) dostajemy,

$$m_2(u) = m_2\left(u^{p^m}\right) = m_2\left(u^{p \cdot p^{m-1}}\right) = [m_2(u^p)]^{p^{m-1}} = 0,$$

a więc analogicznie jak wcześniej $m_1(x) \mid m_2(x)$. Pokazaliśmy zatem, że $m_1(x)$ oraz $m_2(x)$ są stowarzyszone. Pamiętając, że są one również unormowane dostajemy $m_1(x) = m_2(x)$. □

Wniosek 2.2.1:
Niech u będzie elementem pierwotnym $GF(p^m)$. Elementy

$$u, u^p, u^{p^2}, \ldots, u^{p^{m-1}} \in GF(p^m)$$

mają ten sam wielomian minimalny $m(x) \in GF(p)[x]$. Ponadto elementy te są wszystkimi pierwiastkami wielomianu $m(x)$ w ciele $GF(p^m)$.
Dowód:
Wystarczy zastosować powyższe twierdzenie kolejno do par elementów u, u^p; $u^p, u^{p^2}; \ldots; u^{P^{m-2}}, u^{p^{m-1}}$. Druga część wniosku wynika z nierówności $\deg m(x) \leq m$.□

Twierdzenie 2.2.6:
Jeśli $m(x) \in GF(p)[x]$ jest wielomianem minimalnym elementu $u \in GF(p^m)$ takiego, że $\mathrm{rz} u = s$, to

$$m(x) = \prod_{i=0}^{s-1} \left(x - u^{p^i}\right).$$

Dowód:
Łatwo zauważyć, że wielomian $m(x) = \prod_{i=0}^{s-1} \left(x - u^{p^i}\right)$ jest wielomianem unormowanym którego pierwiastkiem jest element u. Pozostaje więc wykazać, że jest to wielomian najniższego stopnia nad ciałem $GF(p)$.

1. Minimalność stopnia $m(x)$.
   Załóżmy, że wielomian $\tilde{m}(x)$ jest unormowanym wielomianem najniższego stopnia o pierwiastku u. Z twierdzenia 2.2.1 wiemy, że dla wielomianów $\tilde{m}(x)$ oraz $m(x)$ zachodzi wówczas

   $$\tilde{m}(x) \mid m(x) \Rightarrow m(x) = q(x)\,\tilde{m}(x) \Rightarrow \deg m(x) = \deg q(x) + \deg \tilde{m}(x).$$

   Zastanówmy się więc, ile wynosi $\deg m(x)$ oraz $\deg \tilde{m}(x)$. Bezpośrednio z postaci wielomianu $m(x)$ widać, że $\deg m(x) \leq s$. Z drugiej jednak strony można zauważyć, że $m\left(u^{p^i}\right) = 0$ dla $i = 0, \ldots, s-1$ oraz $u^{p^i} \neq u^{p^j}$ dla $i, j = 0, \ldots, s-1$, $i \neq j$, gdyż założyliśmy, że $\mathrm{rz} u = s$. Implikuje to $\deg m(x) \geq s$, a więc $\deg m(x) = s$. Pamiętając, że $\tilde{m}(u) = 0$ oraz korzystając z równości $\tilde{m}\left(u^{p^i}\right) = [\tilde{m}(u)]^{p^i}$ możemy, rozumując podobnie jak wcześniej, uzyskać oszacowanie $\deg \tilde{m}(x) \geq s$. Jednak, z uwagi na sposób zdefiniowania $\tilde{m}(x)$, musi zachodzić $\deg \tilde{m}(x) \leq \deg m(x) = s$, a więc również $\deg \tilde{m}(x) = s$. Wstawiając tak uzyskane wartości $\deg m(x)$ oraz $\deg \tilde{m}(x)$ do wcześniej wyprowadzonej równości

   $$\deg m(x) = \deg q(x) + \deg \tilde{m}(x)$$

   dostajemy

   $$\deg q(x) = 0 \Rightarrow q(x) = c \in GF(p^m).$$

   Skoro jednak $\deg m(x) = \deg \tilde{m}(x)$ oraz $m(x)$, $\tilde{m}(x)$ unormowane, więc z uwagi na zachodzącą równość

   $$m(x) = q(x)\,\tilde{m}(x) = c\tilde{m}(x)$$

   musi być $c = 1$, a tym samym $m(x) = \tilde{m}(x)$. $m(x)$ musi więc być wielomianem minimalnego stopnia o pierwiastku u.
2. $m(x) \in GF(p)[x]$
   Niech $m(x) = \sum_{i=0}^{s} u_i x^i$. Obliczymy teraz $[m(x)]^p$ dwoma sposobami. Z jednej strony wiemy już z twierdzenia 1.3.7, że

   $$[m(x)]^p = \sum_{i=0}^{s} u_i^p x^{ip}.$$

Z drugiej strony, korzystając z równoważności $u^{p^i} \equiv u^{p^j} \Leftrightarrow j - i \equiv 0 \,(\mathrm{mod} s)$ oraz z twierdzenia 1.3.7 możemy napisać

$$\begin{aligned}
[m(x)]^p &= \prod_{i=0}^{s-1} \left(x - u^{p^i}\right)^p \\
&= \prod_{i=0}^{s-1} \left(x^p - u^{p^{i+1}}\right) \\
&= \prod_{i=1}^{s} \left(x^p + u^{p^i}\right) \\
&= \prod_{i=0}^{s-1} \left(x^p - u^{p^i}\right) \\
&= m(x^p) \\
&= \sum_{i=0}^{s} u_i x^{ip}.
\end{aligned}$$

Dostaliśmy więc

$$\sum_{i=0}^{s} u_i^p x^{ip} = \sum_{i=0}^{s} u_i x^{ip} \Rightarrow u_i^p = u_i \Rightarrow u_i^p - u_i = 0.$$

Jak pamiętamy, równanie postaci $x^p - x = 0$ spełniane jest przez wszystkie elementy ciała $GF(p)$ (twierdzenie 1.3.5). Zauważając jeszcze, że wyrażenie $x^p - x$ jest wielomianem stopnia p, a więc ma w ciele nie więcej niż p pierwiastków (twierdzenie 1.1.8), dostajemy, że elementy ciała $GF(p)$ są jedynymi rozwiązaniami naszego równania. Pokazaliśmy więc, że elementy $u_i \in GF(p)$. □

2.3. Metody konstrukcji

Metoda I:
Niech u będzie elementem pierwotnym ciała $GF(p^m)$. Z twierdzenia 2.2.6 wiemy, że wielomian minimalny $m(x) \in GF(p)[x]$ elementu pierwotnego u jest wielomianem stopnia m o pierwiastkach $u, u^p, u^{p^2}, \ldots, u^{p^{m-1}}$ postaci

$$m_1(x) = (x-u)\left(x-u^p\right)\left(x-u^{p^2}\right)\ldots\left(x-u^{p^{m-1}}\right).$$

Pamiętając, że wielomian minimalny pewnego elementu $v \in GF(p^m)$ jest również wielomianem minimalnym elementu v^p możemy, biorąc dowolny jeszcze nie wybrany element ciała $GF(p^m)$, wygenerować wszystkie pierwiastki v, v^p, v^{p^2}, $\ldots$, $v^{p^{r-1}}$ wielomianu minimalnego

$$m_2(x) = (x-v)\left(x-v^p\right)\left(x-v^{p^2}\right)\left(x-v^{p^{r-1}}\right),$$

gdzie $\deg m_2(x) = r \mid m$.

Postępując analogicznie możemy wygenerować wielomiany minimalne

$$m_1(x), m_2(x), \ldots, m_l(x)$$

wszystkich elementów ciała $GF(p^m)$. Ostatecznie wymnażając nawiasy oraz korzystając z wiedzy o wielomianach nierozkładalnych nad konkretnym ciałem $\mathbb{Z}_p$ możemy próbować znaleźć współczynniki wielomianów minimalnych już w postaci $m_i(x) = a_0 + a_1 x + \ldots + a_n x^n$.

Wielomiany nierozkładalne stopnia n nad danym ciałem $\mathbb{Z}_p$ najłatwiej jest znaleźć poprzez znalezienie wszystkich wielomianów rozkładalnych (czyli iloczynów wielomianów niższego stopnia), a następnie sprawdzenie, których z wielomianów nie udało się przedstawić w takiej postaci. Wielomiany nierozkładalny nad ciałem $\mathbb{Z}_2$ o stopniach niewiększych niż 4 znajdują się w dodatku 3.1.

Przykład 2.3.1:
Znajdźmy wielomiany minimalne elementów ciała $GF(16) = GF(2^4)$.
Niech u będzie naszym elementem pierwotnym. Elementy u, u^2, u^4, u^8 będą więc miały ten sam wielomian minimalny

$$m_1(x) = (x-u)\left(x-u^2\right)\left(x-u^4\right)\left(x-u^8\right).$$

Biorąc teraz pierwszy jeszcze nie wykorzystany element ciała, mianowicie u^3, możemy skonstruować wielomian minimalny dla u^3, u^6, u^9, u^{12}

$$m_2(x) = \left(x-u^3\right)\left(x-u^6\right)\left(x-u^9\right)\left(x-u^{12}\right).$$

Postępując analogicznie, konstruujemy wielomian minimalny elementów u^5, u^{10}

$$m_3(x) = \left(x-u^5\right)\left(x-u^{10}\right)$$

oraz wielomian minimalny elementów u^7, u^{11}, u^{13}, u^{14}

$$m_4(x) = \left(x-u^7\right)\left(x-u^{11}\right)\left(x-u^{13}\right)\left(x-u^{14}\right).$$

Wymnażając nawiasy oraz przyjmując oznaczenia $\gamma_1 = u+u^2+u^4+u^8$, $\gamma_2 = u^3+u^6+u^9+u^{12}$, $\gamma_3 = u^5+u^{10}$, $\gamma_4 = u^7+u^{11}+u^{13}+u^{14}$ dostajemy wielomiany następującej postaci

$$\begin{aligned}
m_1(x) &= x^4+\gamma_1 x^3+(\gamma_2+\gamma_3)x^2+\gamma_4 x+1,\\
m_2(x) &= x^4+\gamma_2 x^3+\gamma_2 x^2+\gamma_2 x+1,\\
m_3(x) &= x^2+\gamma_3 x+1,\\
m_4(x) &= x^4+\gamma_4 x^3+(\gamma_2+\gamma_3)x^2+\gamma_1 x+1.
\end{aligned}$$

Rozpatrując wielomian $m_3(x)$ oraz pamiętając, że w ciele $\mathbb{Z}_2$ mamy tylko jeden wielomian nierozkładalny stopnia 2 postaci x^2+x+1, możemy przyjąć $\gamma_3 = 1$. Przeanalizujmy teraz sytuację z wielomianem $m_2(x)$. Może on przyjąć postać $m_2(x) = x^4+1$ lub $m_2(x) = x^4+x^3+x^2+x+1$. Przy czym pierwszą z tych postaci możemy rozłożyć na $\left(x^2+1\right)^2$, więc pozostaje nam przyjąć $\gamma_2 = 1$. Pozostały nam więc do rozpatrzenia wielomiany $m_1(x)$ oraz $m_4(x)$ które po dokonanych już obserwacjach mają postać $m_1(x) = x^4+\gamma_1 x^3+\gamma_4 x+1$ oraz $m_4(x) = x^4+\gamma_4 x^3+\gamma_1 x+1$. Z analizy wielomianów nierozkładalnych nad $\mathbb{Z}_2$ możemy w tym wypadku stwierdzić tylko, że $\gamma_1 \neq \gamma_4$. Tak więc ostatecznie dostajemy

$$\begin{aligned}
m_1(x) &= x^4+\gamma_1 x^3+\gamma_4 x+1,\\
m_2(x) &= x^4+x^3+x^2+x+1,\\
m_3(x) &= x^2+x+1,\\
m_4(x) &= x^4+\gamma_4 x^3+\gamma_1 x+1.
\end{aligned}$$

gdzie $\gamma_1 \neq \gamma_4$.

Tak więc udało nam się w ten sposób wyznaczyć dwa wielomiany minimalne oraz przybliżyć postać dwóch kolejnych w dosyć prosty sposób, o ile znamy wszystkie

wielomiany minimalne odpowiednich stopni danego ciała $\mathbb{Z}_p$. Poznamy jednak teraz metodę która w sposób algorytmiczny pozwoli nam wyznaczyć dokładną postać wszystkich wielomianów minimalnych.

Wprowadzimy teraz pewną zależność rekurencyjną stowarzyszoną z wielomianem. Niech więc dany będzie wielomian

$$p(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in GF(q),$$

przyrównując go do zera, otrzymujemy równość postaci

$$x^m = -a_{m-1}x^{m-1} + \ldots + a_1 x + a_0.$$

Interesująca nas zależność rekurencyjna stowarzyszona z naszym wielomianem będzie miała wówczas postać

$$s_{j+m} = -a_{m-1}s_{j+m-1} - \ldots - a_1 x - a_0, j = 0, 1, 2, 3, \ldots.$$

Działania dla powyższej zależności wykonujemy zgodnie z zasadami obowiązującymi w $GF(q)$. Zakładając ciąg początkowy s_0, s_1, ..., s_{m-1} możemy wygenerować za pomocą powyższego wzoru kolejne elementy sekwencji.

Własności jakie tak wygenerowana sekwencja posiada, pozwalają nam na przyporządkowanie każdemu niezerowemu elementowi ciała $GF(p^m)$ wektora o m współrzędnych w następujący sposób:

1. Niech $p(x)$ będzie wielomianem nierozkładalnym nad $\mathbb{Z}_p$ generującym ciało $GF(p^m)$.
2. Znajdujemy zależność rekurencyjną odpowiadającą $p(x)$, przyjmujemy jako wartości początkowe do generowania sekwencji s_0, ..., s_{m-1} (nie wszystkie równ zero) i na podstawie tych wartości generujemy $p^m + m - 2$ elementy sekwencji
$$s_0,\ s_1,\ \ldots,\ s_{p^m+m-3}.$$
3. Przyporządkowujemy elementom ciała $GF(p^m) = \left\{0, 1, u, u^2, \ldots, u^{p^m-2}\right\}$ wektory długości m w następujący sposób:
$0 = [0, 0, \ldots, 0]$,
$1 = [s_0, s_1, \ldots, s_{m-1}]$,
$u = [s_1, s_2, \ldots, s_m]$,
$u^2 = [s_2, s_3, \ldots, s_{m+1}]$,
...,
$u^{p^m-2} = [s_{p^m-2}, s_{p^m-1}, \ldots, s_{p^m+m-3}]$.

Posługując się elementami ciała w postaci wektorów, dużo łatwiej będzie nam dodawać elementy ciała. Reprezentacja taka, jak zaraz się przekonamy, pozwali też łatwo znaleźć współczynniki wielomianów minimalnych.

Metoda II:
Niech dany będzie wielomian nierozkładalny $p(x) \in \mathbb{Z}_p$ taki, że $GF(p^m) = \mathbb{Z}_p/(p(x)) = \left\{0, 1, u, u^2, \ldots, u^{p^m-2}\right\}$. Elementom ciała $GF(p^m)$ możemy, zgodnie z wyżej opisaną procedurą, przyporządkować wektory długości m : $0 = \overrightarrow{0}$, $1 = \overrightarrow{v_1}$, $u = \overrightarrow{v_2}$, ..., $u^{p^m-2} = \overrightarrow{v_{p^m-1}}$. Biorąc dowolny element $w \in GF(p^m)$ i generując wszystkie elementy w, w^p, ..., $w^{p^{r-1}}$ o tym samym wielomianie minimalnym, ustalamy stopień naszego wielomianu $\deg m_1(x) = r$. Znając już stopień wielomianu możemy zapisać go w postaci

$$m_1(x) = x^r + a_{r-1}x^{r-1} + \ldots + a_1 x^1 + a_0,$$

gdzie współczynniki $a_0, \ldots, a_{r-1}$ są nieznane. Dokonując jednak podstawienia

$$w^r + a_{r-1}w^{r-1} + \ldots + a_1 w + a_0 \quad = \quad 0,$$

a następnie przypominając sobie, że dla pewnego $i : w = u^i$, możemy napisać

$$\left(u^i\right)^r + a_{r-1}\left(u^i\right)^{r-1} + \ldots + a_1\left(u^i\right) + a_0 = 0.$$

Podstawiając za elementy $u^{i\cdot k}$, $k = 0, \ldots, r$ odpowiednie wektory dostajemy układ m równań z $r \leq m$ niewiadomymi $a_0, \ldots, a_{r-1}$, którego rozwiązanie pozwoli na wyznaczenie współczynników wielomianu minimalnego.

Przykład 2.3.2:
Rozważmy ciało $GF(16) = GF\left(2^4\right) = \mathbb{Z}_2/\left(x^4 + x + 1\right) = \left\{0, 1, u, u^2, \ldots, u^{14}\right\}$ i znajdźmy w nim wielomian minimalny odpowiadający elementowi u^7. Zależnością rekurencyjną odpowiadającą wielomianowi x^4+x+1 będzie $s_{j+4} = s_{j+1}+s_j$, $j = 0, 1, 2, \ldots$. Przyjmując jako sekwencję początkową 1000 możemy przyporządkować elementom ciała następujące wektory:

$0 = [0,0,0,0]$, $1 = [1,0,0,0]$, $u = [0,0,0,1]$, $u^2 = [0,0,1,0]$, $u^3 = [0,1,0,0]$, $u^4 = [1,0,0,1]$, $u^5 = [0,0,1,1]$, $u^6 = [0,1,1,0]$, $u^7 = [1,1,0,1]$, $u^8 = [1,0,1,0]$, $u^9 = [0,1,0,1]$, $u^{10} = [1,0,1,1]$, $u^{11} = [0,1,1,1]$, $u^{12} = [1,1,1,1]$, $u^{13} = [1,1,1,0]$, $u^{14} = [1,1,0,0]$.

Elementami o tym samym wielomianie minimalnym co u^7 są elementy u^{11}, u^{13}, u^{14}. Tak więc szukany przez nas wielomian $m(x)$ będzie stopnia 4. Zapiszmy go więc w postaci

$$m(x) = x^4 + ax^3 + bx^2 + cx + d.$$

Podstawiając teraz u^7 dostajemy

$$\begin{aligned} \left(u^7\right)^4 + a\left(u^7\right)^3 + b\left(u^7\right)^2 + c\left(u^7\right) + d &= 0, \\ u^{13} + au^6 + bu^{14} + cu^7 + d &= 0. \end{aligned}$$

Zamieńmy więc u^6, u^7, u^{13}, u^{14} na odpowiadające im wektory

$$[1,1,1,0] + a[0,1,1,0] + b[1,1,0,0] + c[1,1,0,1] + d[1,0,0,0] = [0,0,0,0].$$

Powyższe równanie wektorowe prowadzi do układu czterech równań skalarnych postaci

$$\begin{cases} b + c + d = 1 \\ a + b + c = 1 \\ a = 1 \\ c = 0 \end{cases},$$

których rozwiązanie to $a = 1, b = 0, c = 0, d = 1$. Tak więc wielomian minimalny elementu u^7 jest postaci

$$m(x) = x^4 + x^3 + 1.$$

Drugą metodą udało nam się więc uzyskać postać wielomianu, którego pierwszą jednoznacznie nie wyznaczyliśmy.

Rozdział 3

Dodatki

3.1. Wielomiany nierozkładalne nad $\mathbb{Z}_2$

Pierwszego stopnia:
x,
$x+1$.

Drugiego stopnia:
x^2+x+1.

Trzeciego stopnia:
x^3+x^2+1,
x^3+x+1.

Czwartego stopnia:
$x^4+x^3+x^2+x+1$,
x^4+x^3+1,
x^4+x+1.

Bibliografia

[1] T. W. Hungerford, Abstract Algebra: An Introduction
[2] W. Lipski, W. Marek, Analiza Kombinatoryczna, PWN 1986
[3] A. Pilitowska, Skrypt z zajęć Kody Wykrywające i Korygujące Błędy, PW 2007
[4] A. Romanowska, Skrypt z zajęć Algebra i Jej Zastosowania II, PW 2007
[5] T. Świrszcz, Algebra Liniowa z Geometrią Analityczną, OWPW 2004
[6] W. Mochnacki, Kody Korekcyjne i Kryptografia, OWPW 2000