Ciała skończone

1. Ciała: podstawy

Definicja 1. Każdy zbiór liczb, w którym są wykonalne wszystkie cztery działania z wyjątkiem dzielenia przez 0 i który zawiera więcej niż jedną liczbę, nazywamy *ciałem liczbowym.*

Definicja 2. Niech będzie dany zbiór K, w którym są określone dwa działania $\oplus$ i $\odot$ zwane odpowiednio dodawaniem i mnożeniem. Jeżeli dla dowolnych $x, y, z \in K$ i dla pewnych elementów $0, 1 \in K$ mamy:

1. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ (dodawanie jest łączne),
2. $x \oplus y = y \oplus x$ (dodawanie jest przemienne),
3. $0 \oplus x = x \oplus 0 = x$ (istnieje w K element zerowy 0),
4. $x \oplus (-x) = 0$ (dla każdego elementu x istnieje element przeciwny $-x$),
5. $(x \odot y) \odot z = x \odot (y \odot z)$ (mnożenie jest łączne),
6. $x \odot y = y \odot x$ (mnożenie jest przemienne),
7. $1 \odot x = x \odot 1 = x$ (istnieje w K element jednostkowy $1 \neq 0$),
8. $x \odot x^{-1} = x^{-1} \odot x = 1$ (dla $x \neq 0$ istnieje element odwrotny x^{-1}),
9. $x \odot (y \oplus z) = x \odot y \oplus x \odot z$ (mnożenie jest rozdzielne względem dodawania),

to system $(K, \oplus, \odot)$ nazywamy *ciałem (abstrakcyjnym).*

Przykłady

1. Ciała liczbowe $\mathbb{Q}$, $\mathbb{R}$, $\{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$.

2. Niech p będzie liczbą pierwszą. Rozpatrzmy zbiór $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ możliwych reszt z dzielenia przez p. W zbiorze tym wprowadzimy działania *dodawania i mnożenia modulo p.* Określone są one następująco:

$$a + b = \text{ reszta z dzielenia zwykłej sumy przez } p,$$

$$a \cdot b = \text{ reszta z dzielenia zwykłego iloczynu przez } p.$$

Piszemy $a + b = c (\mathrm{mod}\, p)$. Na przykład:

$$2 + 2 = 1 (\mathrm{mod}\, 3),\ 2 \cdot 2 = 1 (\mathrm{mod}\, 3),\ 3 + 4 = 2 (\mathrm{mod}\, 5),\ 3 \cdot 2 = 1 (\mathrm{mod}\, 5).$$

Struktura $(\mathbf{Z}_p, +, \cdot)$ jest ciałem (ale nie liczbowym, bo to nie są zwykłe działania arytmetyczne).

Zbiory $\mathbb{Z}_p$ są skończone, więc można sporządzić dla nich kompletne tabelki działań. Przykładowo dla $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

oraz dla $\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

.

Z tabel widzimy, że np. $-2 = 1 (\mathrm{mod}\, 3)$, $2^{-1} = 2 (\mathrm{mod}\, 3)$.

3. Ciało funkcji wymiernych. *Funkcją wymierną* jednej zmiennej nazywamy iloraz dwóch wielomianów, tzn. funkcję postaci:

$$f(x) = \frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m}.$$

Zbiór wszystkich takich funkcji oznaczymy przez $\mathbb{R}(x)$. Zwykłe działania (dodawanie i mnożenie funkcji) określają w tym zbiorze strukturę ciała.

Definicja 3. Przekształcenie $f : K \longrightarrow K'$ odwzorowujące wzajemnie jednoznacznie ciało K na ciało K' i zachowujące działania, tj.:

$$f(a+b) = f(a) \oplus f(b), f(ab) = f(a) \odot f(b) \text{ dla } a, b \in K,$$

nazywamy *izomorfizmem.* Ciała K i K' nazywają się *ciałami izomorficznymi.*

Przykłady.
1. Niech $K = K' = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Odwzorowanie $f : K \longrightarrow K'$ dane wzorem $f(a + b\sqrt{2}) = a - b\sqrt{2}$ jest izomorfizmem.
2. Niech $\mathbb{R}(x)$ i $\mathbb{R}(y)$ oznaczają ciała funkcji wymiernych zmiennej x i y odpowiednio. Przyporządkowanie:

$$\frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m} \longleftrightarrow \frac{a_0 + a_1 y + \cdots + a_n y^n}{b_0 + b_1 y + \cdots + b_m y^m}$$

jest izomorfizmem.

2. Podciało i rozszerzenie ciała

Definicja 4. Podzbiór K ciała L, zawierający 0 i 1 i taki, że wykonalne są w nim działania dodawania, odejmowania, mnożenia i dzielenia przez element różny od 0, nazywamy *podciałem.* Ciało L nazywamy wtedy *rozszerzeniem* ciała K.

Definicja 5. Ciało, które nie zawiera żadnego podciała właściwego, nazywamy *ciałem prostym.*

Twierdzenie 1. (twierdzenie o podciele prostym) *Każde ciało K zawiera dokładnie jedno ciało proste K_0. Ciało K_0 jest izomorficzne z ciałem $\mathbb{Q}$ albo z ciałem $\mathbb{Z}_p$ dla pewnej liczby pierwszej p.*

D o w ó d. Rozważmy rodzinę $\mathcal{A}$ wszystkich podciał ciała K. Ponieważ $K \in \mathcal{A}$, więc rodzina $\mathcal{A}$ jest niepusta. Niech K_0 oznacza część wspólną podciał rodziny $\mathcal{A}$. K_0 jest ciałem. Krótkie uzasadnienie: jeśli $x, y \in K_0$, to $x, y \in L$ dla każdego $L \in \mathcal{A}$, zatem $x - y \in L$ i $x/y \in L$, a więc $x - y \in K_0$ i $x/y \in K_0$. K_0 jest ciałem prostym, bo gdyby istniało ciało $M \subset K_0$, $M \neq \mathbf{K}_0$, to M należałoby do $\mathcal{A}$ i część wspólna podciał rodziny $\mathcal{A}$ byłaby mniejsza od K_0. Wreszcie gdyby istniało inne podciało proste K_1 ciała K, to część wspólna $K_0 \cap K_1$ byłaby podciałem ciała K zawartym w K_0, co jest niemożliwe. To kończy pierwszą część twierdzenia.
Drugą część wykażemy konstruując podciało proste danego ciała. Załóżmy, że istnieje taka liczba r, że dla dowolnego $m \in K$ jest $rm = 0$, i niech p będzie najmniejszą liczbą naturalną o tej własności. Wtedy zbiór

$$\{k \cdot 1 : k = 0, 1, \ldots, p-1\}$$

tworzy ciało izomorficzne z $\mathbb{Z}_p$. Jeśli w ciele K nie istnieje taka liczba r, że dla dowolnego $m \in K$ jest $rm = 0$, to elementy $n \cdot 1$, $n \in \mathbb{Z}$, należą do K i są dla $n \neq 0$ różne od zera. Ponieważ w ciele jest wykonalne dzielenie, więc do K należą także wszystkie ułamki w postaci $\frac{n \cdot 1}{m \cdot 1}$,$m \neq 0$. Zbiór tych ułamków jest, jak łatwo sprawdzić, ciałem izomorficznym z $\mathbb{Q}$. □

Definicja 6. [charakterystyki ciała] Mówimy, że *charakterystyką ciała K* jest 0, jeśli ciało proste ciała K jest izomorficzne z ciałem $\mathbb{Q}$. W przeciwnym razie istnieje liczba pierwsza p taka, że ciało proste ciała K jest izomorficzne z ciałem $\mathbb{Z}_p$ i wtedy mówimy, że charakterystyka ciała K jest równa p.

Piszemy: $\mathrm{char}(K)$.
Ciała $\mathbb{R}$ i $\mathbb{C}$ mają charakterystykę 0.
Potrzeba rozszerzania ciał bierze się z obliczania pierwiastków wielomianów.
Przykład. Wielomian x^2-2 nie ma pierwiastków w $\mathbb{Q}$. Jeśli rozszerzymy ciało $\mathbb{Q}$ dołączając do niego $\sqrt{2}$ i wszystkie liczby, które można otrzymać z tego pierwiastka przez działania wymierne, otrzymamy ciało

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \quad a, b \in \mathbb{Q}\}$$

w którym równanie $x^2 - 2 = 0$ ma już rozwiązanie.
Jest to przykład ogólniejszej **metody konstruowania ciał**, którą teraz opiszemy.
Niech a będzie pierwiastkiem wielomianu nierozkładalnego p stopnia n o współczynnikach z ciała K. Mówimy wtedy, że a jest *elementem algebraicznym* nad ciałem K stopnia n. Wielomian p, o którym możemy założyć, że jego najwyższy współczynnik jest równy 1, nazywamy *wielomianem minimalnym* elementu a.
Symbolem $K(a)$ oznaczymy najmniejsze rozszerzenie ciała K zawierające element a.
Z jakich elementów składa się $K(a)$? Ze względu na to, że w ciele muszą być wykonalne działania dodawania, odejmowania, mnożenia i dzielenia, $K(a)$ musi zawierać wszystkie elementy postaci:

$$c_0 + c_1 a + \cdots c_k a^k \ , \ , c_i \in K. \tag{1}$$

Okazuje się, że możemy ograniczyć się do wykładników k mniejszych od n. Jeśli bowiem b jest elementem postaci:

$$c_0 + c_1 a + \cdots c_k a^k, \quad k \geqslant n,$$

to rozważmy wielomian:

$$g = c_0 + c_1 x + \cdots c_k x^k.$$

Podzielmy g przez wielomian minimalny p elementu a:

$$g = qp + r, \quad \deg r < n, \quad r = d_0 + d_1 x + \cdots + d_{n-1} x^{n-1}.$$

Mamy wtedy

$$b = g(a) = q(a)p(a) + r(a) = r(a),$$

czyli $g(a) = r(a)$.
Zatem dowolny element ciała $K(a)$ dający się przedstawić w postaci (1) przedstawia się w postaci:

$$c_0 + c_1 a + \cdots c_k x^k, \quad k < n. \tag{2}$$

Lemat 1. *Zbiór elementów w postaci (2) z działaniami dodawania i mnożenia modulo wielomian p jest ciałem.*

D o w ó d. Wystarczy stwierdzić, że różnica oraz iloraz elementów o postaci (2) też są elementami tej postaci. Dla różnicy jest to oczywiste. Aby wykazać, że iloraz dwóch wyrażeń rozważanej postaci też ma tę postać, wystarczy stwierdzić, że jeśli

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

to odwrotność:

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

też jest elementem tej postaci.
Niech $g = c_0 + c_1 x + \cdots c_{n-1} x^{n-1}$. Wielomian g jest względnie pierwszy z wielomianem minimalnym p elementu a (bo p jest nierozkladalny). Zatem na mocy algorytmu Euklidesa istnieją wielomiany ϕ i ψ, dla których:

$$\phi p + \psi g = 1.$$

Ale $p(a) = 0$, więc $\psi(a)g(a) = 1$, czyli $g(a)^{-1} = \psi(a)$, gdzie $\psi(a) = d_0 + d_1 a + \cdots + d_k a^k$, przy czym można założyć, że $k < n$. Wykazaliśmy więc, że zbiór

$$\{c_0 + c_1 a + \cdots c_k x^k \mid c_i \in K\}$$

zawiera ciało K i element a. Jest to oczywiście najmniejsze ciało o tej własności, czyli jest to $K(a)$.
Przykład. Dla liczby niewymiernej $\sqrt[3]{2}$ wielomianem minimalnym nad $\mathbb{Q}$ jest $x^3 - 2$. Rozszerzenie ciała $\mathbb{Q}$ o ten pierwiastek to:

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \quad , a, b, c \in \mathbb{Q}\}.$$

W tym nowym ciele nadal nie ma rozwiązania np. równanie $x^2 - 3 = 0$, a więc można je dalej rozszerzyć.
Rozszerzenie ciała jako przestrzeń wektorowa.
Ponieważ $K(a) = \{c_0 + c_1 a + \cdots c_{n-1} x^{n-1} \mid c_i \in K\}$, więc $K(a)$ można traktować jako przestrzeń wektorową n–wymiarową nad ciałem K. Układ elementów :

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

stanowi bazę tej przestrzeni. Oczywiście nie jest to jedyna baza, np. dla $\mathbb{Q}(\sqrt{2})$ oprócz bazy $\{1, \sqrt{2}\}$ można rozpatrywać bazę $\{\frac{1+\sqrt{2}}{2}, \frac{1-\sqrt{2}}{2}\}$, bo $a + b\sqrt{2} = (a+b)\frac{1+\sqrt{2}}{2} + (a-b)\frac{1-\sqrt{2}}{2}$, a także inne bazy.
Ogólniej, rozpatrzmy rozszerzenie $K \subset L$.

Definicja 7. *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.

Twierdzenie 2. *Dla każdego rozszerzenia $K \subset L$ istnieje baza. Każde dwie bazy tego samego rozszerzenia są równoliczne.*

Jesli baza jest skończona, to liczbę jej elementów nazywamy *stopniem rozszerzenia* i oznaczamy $[L : K]$. Można wykazać, że $[K(a) : K] = \deg p$, gdzie p jest wielomianem minimalnym elementu a.

3. Ciała skończone

Lemat 2. *Niech F będzie ciałem skończonym, będącym rozszerzeniem q-elementowego ciała K. Wtedy F ma q^m elementów, gdzie $m = [F : K]$.*

D o w ó d. Ciało F można traktować jak przestrzeń liniową nad ciałem K, a ponieważ ciało F jest skończone, więc przestrzeń jest skończenie wymiarowa, np. $\dim F = m$. Jeśli $b_1, b_2, \ldots, b_m$ jest bazą tej przestrzeni, to każdy element można jednoznacznie zapisać w postaci $a_1 b_1 + a_2 b_2 + \cdots + a_m b_m$, gdzie każdy współczynnik a_i, jako element ciała K może przyjmować q wartości. Zatem F składa się z q^m elementów.

Twierdzenie 3. *Niech F będzie ciałem skończonym. Wtedy F składa się z p^n elementów, gdzie $p = \mathrm{char}(F)$, a $n = [F : \mathbb{Z}_p]$.*

D o w ó d. Ponieważ ciało F jest skończone, więc jego charakterystyka jest liczbą pierwszą, a więc jego podciało proste jest izomorficzne z pewnym ciałem $\mathbb{Z}_p$. Na mocy poprzedniego lematu liczba elementów ciała F jest potęgą p.

Lemat 3. *Jeśli F jest ciałem q-elementowym, to dla dowolnego $a \in F$ jest $a^q = a$.*

D o w ó d. Równość jest oczywista dla $a = 0$. Natomiast elementy niezerowe ciała tworzą grupę multiplikatywną rzędu $q-1$, a więc $a^{q-1} = 1$ dla $a \neq 0$. Stąd $a^q = a$.

Lemat 4. *Jeśli F jest ciałem q-elementowym, a K podciałem ciała F, to wielomian $x^q - x \in K[x]$ rozkłada się na czynniki liniowe w $F[x]$:*

$$x^q - x = \Pi_{a \in F}(x - a).$$

Tak więc F jest ciałem rozkładu wielomianu $x^q - x$ nad K.

D o w ó d. Z poprzedniego lematu każdy element a ciała F jest pierwiastkiem wielomianu $x^q - x$, a więc wielomian dzieli się przez $x - a$.

Twierdzenie 4. *Jeżeli p jest wielomianem nierozkładalnym stopnia m nad q-elementowym ciałem K, to klasy reszt modulo p, tj. elementy pierścienia ilorazowego $K[x]/(p)$ tworzą ciało rzędu q^m.*

D o w ó d. Klasy reszt modulo p można utożsamiać z wielomianami

$$c_0 + c_1 x + \cdots c_{m-1} x^{m-1}.$$

Działania na tych wielomianach wykonujemy $\mod p$, tzn. "zwykły" wynik mnożenia czy dodawania dzielimy przez p; reszta z tego dzielenia jest wynikiem $\mod p$. Każdy współczynnik wielomianu można wybrać na q sposobów, więc jest q^m wielomianów, czyli elementów ciała.

Wniosek 1. *Jeżeli istnieje wielomian nierozkładalny stopnia m nad ciałem $\mathbb{Z}_p$, to istnieje ciało rzędu p^m.*

Przykład. Skonstruować ciało 9-elementowe.
Ponieważ $9 = 3^2$, więc to ciało ma charakterystykę 3. Potrzebny jest wielomian nierozkładalny nad $\mathbb{Z}_3$ stopnia 2, np. $x^2 + 1$. Niech a będzie pierwiastkiem tego wielomianu. Rozszerzenie o ten pierwiastek jest ciałem klas reszt $\mod x^2 + 1$, czyli zbiorem

$$\{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}.$$

Wygodniej jest podstawić $x = a$ i wtedy mamy ciało

$$\{0, 1, 2, a, a + 1, a + 2, 2a, 2a + 1, 2a + 2\},$$

gdzie przy wykonywaniu działań ($\mod 3$) należy uwzględnić, że $a^2 + 1 = 0$ (czyli $a^2 = 2$). Np. $2a(2a + 1) = a^2 + 2a = 2a + 2$.
Mamy także: $(2a)^2 + 1 = a^2 + 1 = 0$, co oznacza, że $2a$ jest drugim pierwiastkiem wielomianu $x^2 + 1$, a więc $x^2 + 1 = (x - a)(x - 2a)$.
U w a g a. Ponieważ grupa multiplikatywna ciała jest cykliczna, więc elementy ciała można zapisać w postaci

$$\{0, a, a^2, \ldots, a^8\}.$$

Można też zapisać elementy ciała używając współrzędnych względem bazy $1, a$. Np. $a^7 = (a^2)^3 a = 2^3 a = 2a = (0, 2)$.
Przykład. Wyznaczyć ciało rozkładu wielomianu $x^3 + x + 1$ nad $\mathbb{Z}_2$.
Przykład. Skonstruować ciało $GF(16) = GF(2^4)$ następująco:
a) znaleźć wielomian nierozkładalny stopnia 4; (można to zrobić wypisując kolejno wielomiany stopnia 1, 2, 3 i obliczając ich iloczyny; wielomian, który nie da się otrzymać w ten sposób, jest nierozkładalny;
b) wybrać dowolny z tych wielomianów; oznaczmy go $p(x)$;
c) ciało $GF(16)$ można reprezentować przez klasy reszt wielomianów modulo $p(x)$; mnożeniu elementów ciała odpowiada mnożenie wielomianów, po którym następuje redukcja iloczynu modulo $p(x)$.
Rozwiązanie. Wygenerujemy $GF(16)$ wykorzystując nierozkładalny wielomian $x^4 + x + 1$ i jego pierwiastek α. W bazie $1, \alpha, \alpha^2, \alpha^3$ mamy następującą reprezentację niezerowych elementów ciała:

1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
1	0	0	0	1	0	0	1	1	0	1	0	1	1	1
0	1	0	0	1	1	0	1	0	1	1	1	1	0	0
0	0	1	0	0	1	1	0	1	0	1	1	1	1	0
0	0	0	1	0	0	1	1	0	1	0	1	1	1	1

W zapisie tabeli uwzględniliśmy, że (działania są $\bmod 2$ oraz $\alpha^4 = \alpha + 1$):

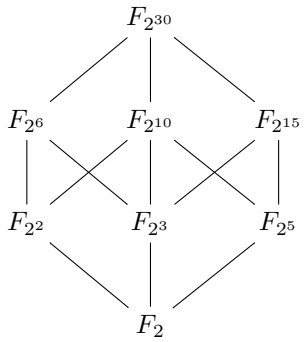
$$\begin{aligned}\alpha^{15} &= (\alpha^4)^3\alpha^3 = (\alpha+1)^3\alpha^3 = (\alpha^3+\alpha^2+\alpha+1)\alpha^3 = \alpha^6+\alpha^5+\alpha^4+\alpha^3 = \\ &= \alpha^4(\alpha^2+\alpha+1)+\alpha^3 = (\alpha+1)(\alpha^2+\alpha+1)+\alpha^3 = 1.\end{aligned}$$

Twierdzenie 5. (istnienie i jednoznaczność ciał skończonych) *Dla dowolnej liczby pierwszej p i dowolnej liczby naturalnej n istnieje ciało skończone o p^n elementach. Dowolne ciało skończone o $q = p^n$ elementach jest izomorficzne z ciałem rozkładu wielomianu $x^q - x$ nad ciałem $\mathbb{F}_p$.*

Dowód pomijamy.

Twierdzenie 6. (kryterium podciała) *Niech $\mathbb{F}_q$ będzie ciałem o $q = p^n$ elementach, gdzie p jest liczbą pierwszą. Wtedy każde podciało ciała $\mathbb{F}_q$ ma rząd p^m, gdzie m jest dodatnim dzielnikiem liczby n. Odwrotnie, jeśli m jest dodatnim dzielnikiem liczby n, to istnieje dokładnie jedno podciało $\mathbb{F}_q$ o p^m elementach.*

Twierdzenie zilustrujemy na przykładzie ciała $F_{2^{30}}$. Liczba 30 ma dzielniki $1, 2, 3, 5, 6, 10, 15$, więc struktura podciał jest następująca.



Ze względu na zastosowania ważne jest następne twierdzenie.

Twierdzenie 7. *Multiplikatywna grupa $\mathbb{F}_q^*$ niezerowych elementów ciała skończonego $\mathbb{F}_q$ jest cykliczna.*

Ponieważ, jak wiadomo, liczba różnych generatorów grupy cyklicznej rzędu n jest równa $\varphi(n)$ (gdzie $\varphi(n)$ jest funkcją Eulera), więc grupa $\mathbb{F}_q^*$ ma $\varphi(q-1)$ różnych generatorów.

Definicja 8. *Generator grupy cyklicznej $\mathbb{F}_q^*$ nazywamy* elementem prymitywnym *ciała $\mathbb{F}_q$.*

Twierdzenie 8. *Niech $\mathbb{F}_q$ będzie ciałem skończonym, a $\mathbb{F}_r$ jego skończonym rozszerzeniem. Wtedy $\mathbb{F}_r$ jest rozszerzeniem algebraicznym prostym ciała $\mathbb{F}_q$, przy czym generatorem tego rozszerzenia może być dowolny element prymitywny ciała $\mathbb{F}_r$.*

Wniosek 2. *Dla dowolnego skończonego ciała $\mathbb{F}_q$ i dowolnej liczby naturalnej n w pierścieniu $\mathbb{F}_q[x]$ istnieje nieprzywiedlny (tj. nierozkładalny) wielomian stopnia n.*

4. Pierwiastki z 1 i wielomiany cyklotomiczne

Definicja 9. *Niech $n \in \mathbb{N}$. Ciało rozkładu wielomianu $x^n - 1$ nad ciałem K nazywamy n-tym* ciałem podziału koła *lub n-tym ciałem cyklotomicznym nad K i oznaczamy $K^{(n)}$. Pierwiastki tego wielomianu w ciele $K^{(n)}$ nazywamy pierwiastkami z jedności stopnia n; zbiór tych pierwiastków oznaczamy $E^{(n)}$.*

Twierdzenie 9. *Niech $n \in \mathbb{N}$ i niech K będzie ciałem charakterystyki p. Wtedy: (i) Jeżeli p nie dzieli n, to zbiór $E^{(n)}$ jest podgrupą cykliczną rzędu n grupy multiplikatywnej ciała $K^{(n)}$.*

(ii) Jeżeli p dzieli n i $n = mp^e$, gdzie $m, e \in \mathbb{N}$ oraz p nie dzieli m, to $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ i pierwiastkami wielomianu $x^n - 1$ w ciele $K^{(n)}$ są wszystkie elementy zbioru $E^{(m)}$, z których każdy ma krotność p^e.

Definicja 10. *Niech K będzie ciałem charakterystyki p, a n niech będzie liczbą naturalną nie dzielącą sie przez p. Wtedy generator grupy cyklicznej $E^{(n)}$ nazywamy* pierwiastkiem pierwotnym *(albo prymitywnym) z jedności stopnia n nad ciałem K.*

Jeżeli p nie dzieli n, to istnieje dokładnie $\varphi(n)$ różnych pierwiastków pierwotnych stopnia n nad ciałem K. Jeśli ζ jest jednym z nich, to wszystkie pierwiastki pierwotne z jedności stopnia n nad ciałem K są postaci ζ^s, gdzie $1 \leqslant s \leqslant n$ oraz $(s, n) = 1$.

Definicja 11. *Niech K będzie ciałem charakterystyki p, n niech będzie liczbą naturalną nie dzielącą się przez p, a ζ - pierwiastkiem pierwotnym z jedności stopnia n nad K . Wtedy wielomian*

$$Q_n(x) = \prod_{s=1,(s,n)=1}^{n} (x - \zeta^s)$$

nazywamy n-tym wielomianem cyklotomicznym *(lub* wielomianem podziału koła*) nad ciałem K.*

Twierdzenie 10. *Niech K - ciało charakterystyki p, n - liczba naturalna nie dzieląca się przez p. Wtedy*
(i) $x^n - 1 = \prod_{d|n} Q_d(x)$;
(ii) współczynniki n-tego wielomianu cyklotomicznego $Q_n(x)$ należą do podciała prostego ciała K gdy p jest liczbą pierwszą, albo do pierścienia $\mathbb{Z}$ gdy $p = 0$.

Powyższe twierdzenie pozwala wyznaczyć niektóre wielomiany.
Przykład. Niech r będzie liczbą pierwszą, $n \in \mathbb{N}$. Wtedy

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{Q_1(x)Q_r(x)\dots Q_{r^{k-1}}(x)} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1},$$

czyli

$$Q_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \dots + x^{(r-1)r^{k-1}}.$$

W szczególności $Q_r(x) = 1 + x + x^2 + \dots + x^{(r-1)}$.

Twierdzenie 11. *Ciało podziału koła $K^{(n)}$ jest prostym rozszerzeniem algebraicznym ciała K. Ponadto:*
(i) Jeśli $K = \mathbb{Q}$, to $[K^{(n)} : K] = \varphi(n)$, przy czym wielomian cyklotomiczny Q_n jest nieprzywiedlny nad K;
(ii) Jeśli $K = \mathbb{F}_q$ i $NWD(q, n) = 1$, to $[K^{(n)} : K] = d$, gdzie d jest najmniejszą liczba naturalną taką, że $q^d \equiv 1(\mod n)$. Przy tym wielomian cyklotomiczny Q_n rozkłada się na iloczyn $\varphi(n)/d$ różnych unormowanych i nieprzywiedlnych wielomianów z $K[x]$ tego samego stopnia d, i $K^{(n)}$ jest ciałem rozkładu każdego z tych wielomianów.

Twierdzenie 12. *Ciało skończone $\mathbb{F}_q$ jest $(q-1)$-szym ciałem cyklotomicznym nad dowolnym ze swoich podciał.*

Ponieważ $\mathbb{F}_q^*$ jest cykliczną grupą rzędu $q-1$, to dla dowolnego dodatniego dzielnika n liczby $q-1$ istnieje cykliczna podgrupa $\{1, \alpha, \dots, \alpha^{n-1}\}$ rzędu n grupy $\mathbb{F}_q^*$. Wszystkie elementy tej grupy są pierwiastkami n-tego stopnia z jedności nad dowolnym podciałem ciała $\mathbb{F}_q$, a jej generator α jest pierwiastkiem pierwotnym n-tego stopnia z jedności nad dowolnym podciałem ciała $\mathbb{F}_q$.