Ciała i wielomiany

1 Definicja ciała

Niech F będzie zbiorem, i niech $+$ („dodawanie") oraz $\cdot$ („mnożenie") będą działaniami na zbiorze F.

Definicja. Zbiór F wraz z działaniami $+$ i $\cdot$ nazywamy *ciałem*, jeśli są spełnione następujące własności:

(C1) $(F, +)$ jest grupą abelową (element neutralny dla działania $+$ oznaczamy przez 0, i nazywamy *zerem*, zaś element odwrotny do a względem działania $+$ oznaczamy przez $-a$, i nazywamy *elementem przeciwnym* do a);

(C2) $(F \setminus \{0\}, \cdot)$ jest grupą abelową (element neutralny dla działania $\cdot$ oznaczamy przez 1, i nazywamy *jedynką*, zaś element odwrotny do $a \neq 0$ względem działania $\cdot$ oznaczamy przez a^{-1}, i nazywamy *odwrotnością* a);

(C3) mnożenie jest *rozdzielne* względem dodawania, tzn. dla dowolnych $a, b, c \in F$ zachodzi
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

Zamiast $a \cdot b$ piszemy zwykle ab. Zamiast ab^{-1} piszemy zwykle a/b lub $\frac{a}{b}$. Dalej, mnożenie wiąże mocniej niż dodawanie, tzn. $ab + c$ oznacza $(a \cdot b) + c$.

Dla $n \in \mathbb{N}$ i $a \in F$ oznaczamy

$$na := \underbrace{a + \ldots + a}_{n \text{ składników}}, \qquad (-n)a := \underbrace{(-a) + \ldots + (-a)}_{n \text{ składników}}.$$

Ponadto, $0 \cdot a := 0$ dla dowolnego $a \in F$.

Dla $n \in \mathbb{N}$ i $a \in F$ oznaczamy

$$a^n := \underbrace{a \cdot \ldots \cdot a}_{n \text{ czynników}},$$

a jeśli ponadto $a \neq 0$, to oznaczamy

$$a^{-n} := \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{n \text{ czynników}}.$$

Zachodzą następujące równości:

- $(-k)a = -(ka)$, dla dowolnych $k \in \mathbb{Z}$ i $a \in F$ (zatem zwykle piszemy $-ka$);
- $(k+l)a = ka + la$, dla dowolnych $k, l \in \mathbb{Z}$ i $a \in F$;
- $k(a+b) = ka + kb$, dla dowolnych $k \in \mathbb{Z}$ i $a, b \in F$;
- $k(a \cdot b) = (ka) \cdot b$, dla dowolnych $k \in \mathbb{Z}$ i $a, b \in F$;
- $a^{k+l} = a^k \cdot a^l$, dla dowolnych $k, l \in \mathbb{Z}$ i $a \in F$, $a \neq 0$.

We wszystkich ciałach zachodzą też standardowe wzory skróconego mnożenia i wzór na dwumian Newtona. Jednakże, w **konkretnych** ciałach mogą one mieć uproszczoną postać (patrz przykład w rozdziale o ciałach $\mathbb{Z}_p$ poniżej).

Definicja. *Charakterystyką* ciała $(F, +, \cdot)$ nazywamy najmniejszą liczbę naturalną p taką, że $pa = 0$ dla dowolnego $a \in F \setminus \{0\}$. Jeśli nie ma takiej liczby, mówimy, że ciało jest charakterystyki zero.

Dość łatwo wykazać, że (niezerowa) charakterystyka ciała musi być liczbą pierwszą.

Przykład 1. $(\mathbb{Q}, +, \cdot)$, gdzie $\mathbb{Q}$ jest zbiorem wszystkich liczb wymiernych, $+$ jest działaniem dodawania i $\cdot$ jest działaniem mnożenia, jest ciałem. Jest to ciało charakterystyki zero.

Przykład 2. $(\mathbb{R}, +, \cdot)$, gdzie $\mathbb{R}$ jest zbiorem wszystkich liczb rzeczywistych, $+$ jest działaniem dodawania i $\cdot$ jest działaniem mnożenia, jest ciałem. Jest to ciało charakterystyki zero.

Przykład 3. $(\mathbb{C}, +, \cdot)$, gdzie $\mathbb{C}$ jest zbiorem wszystkich liczb zespolonych, $+$ jest działaniem dodawania i $\cdot$ jest działaniem mnożenia, jest ciałem. Jest to ciało charakterystyki zero.

Przykład 4. $(\mathbb{R}(x), +, \cdot)$, gdzie $\mathbb{R}(x)$ jest zbiorem wszystkich funkcji wymiernych jednej zmiennej rzeczywistej x, $+$ jest działaniem dodawania i $\cdot$ jest działaniem mnożenia, jest ciałem. Jest to ciało charakterystyki zero.

2 Ciało $\mathbb{Z}_2$

Niech $\mathbb{Z}_2$ oznacza zbiór $\{0, 1\}$. Zdefiniujmy „dodawanie” na $\mathbb{Z}_2$ wzorem

$$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0,$$

i zdefiniujmy „mnożenie” na $\mathbb{Z}_2$ wzorem

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

Powyżej zdefiniowane operacje nazywamy, odpowiednio, *dodawaniem* (*mnożeniem*) *modulo* 2.

$(\mathbb{Z}_2, +, \cdot)$ jest ciałem (nazywanym *ciałem reszt modulo* 2). Zwykle ciało reszt modulo 2 zapisujemy po prostu $\mathbb{Z}_2$.

Zauważmy, że $\mathbb{Z}_2$ jest ciałem charakterystyki dwa. Wynika stąd w szczególności, że w $\mathbb{Z}_2$ zachodzi $-1 = 1$.

3 Ciało $\mathbb{Z}_p$

Niech $\mathbb{Z}_p$, gdzie p jest **liczbą pierwszą**, oznacza zbiór $\{0, 1, 2, \ldots, p-1\}$. Dla $a, b \in \mathbb{Z}_p$ zdefiniujmy „sumę" $a + b$ jako resztę z dzielenia „zwykłej" sumy liczb a i b przez p, i „iloczyn" $a \cdot b$ jako resztę z dzielenia „zwykłego" iloczynu liczb a i b przez p. Operacje te nazywamy, odpowiednio, *dodawaniem modulo* p i *mnożeniem modulo* p.

Okazuje się, że zbiór $\mathbb{Z}_p$ wraz z działaniami dodawania i mnożenia modulo p jest ciałem. To, że zachodzi łączność i przemienność dodawania i mnożenia modulo p, jak i rozdzielność, jest (niemal) oczywiste. Elementem neutralnym dodawania jest 0, elementem neutralnym mnożenia jest 1.

Trochę mniej oczywiste jest istnienie elementu przeciwnego dla $a \in \mathbb{Z}_p$. Zauważmy, że $p - a \in \mathbb{Z}_p$ i że „zwykła" suma a i $p - a$ to p. Zatem dodanie modulo p elementów a i $p - a$ da nam zero.

Rzeczą zupełnie nieoczywistą jest istnienie, dla każdego niezerowego $a \in \mathbb{Z}_p$, jego odwrotności. Zastanówmy się, co to znaczy. Otóż a^{-1} ma to być taka liczba b ze zbioru $\{1, 2, \ldots, p-1\}$, że „zwykły" iloczyn a i b ma, po podzieleniu przez p, dawać resztę 1. Innymi słowy, trzeba znaleźć takie liczby $b \in \{1, 2, \ldots, p-1\}$ i $n \in \mathbb{N}$, że $ab = np + 1$ (tutaj wszystkie działania są „zwykłe"). A że coś takiego można zrobić, wynika z pewnego twierdzenia z teorii liczb, które podaję bez dowodu:

Twierdzenie 1. *Dla liczb naturalnych a i b istnieją takie liczby całkowite m, n, że $ma + nb$ jest równe największemu wspólnemu dzielnikowi liczb a i b.*

$(\mathbb{Z}_p, +, \cdot)$ nazywamy *ciałem reszt modulo* p. Zwykle ciało reszt modulo p zapisujemy po prostu $\mathbb{Z}_p$.

$\mathbb{Z}_p$ jest ciałem charakterystyki p.

Przykład. Zastanówmy się, jak wygląda wzór skróconego mnożenia

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

w ciele $\mathbb{Z}_3$. Jako że jest to ciało charakterystyki 3, drugi i trzeci składnik po prawej stronie powyższego wzoru redukują się do zera, czyli mamy:

$$(a+b)^3 = a^3 + b^3.$$

4 Wielomiany

Definicja. *Wielomianem* zmiennej x nad ciałem F nazywamy wyrażenie

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

gdzie $a_0, \ldots, a_n \in F$ i $n \in \mathbb{N} \cup \{0\}$.

Element a_i nazywamy *współczynnikiem* przy x^i w $P(x)$. Zamiast $1 \cdot x^k$ piszemy po prostu x^k.

Gdy n jest największą liczbą taką, że $a_n \neq 0$, mówimy, że wielomian $P(x)$ ma *stopień* n (i zapisujemy $\operatorname{st} P(x) = n$). Gdy wszystkie współczynniki w $P(x)$ są zerami, wielomian $P(x)$ nazywamy *wielomianem zerowym*. Umawiamy się, że stopień wielomianu zerowego to $-\infty$.

Wielomian zerowy i wielomiany stopnia zero nazywamy *wielomianami stałymi*.

Zbiór wszystkich wielomianów zmiennej x nad ciałem F oznaczamy przez $F[x]$.

Definicja. Wielomiany $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ i $R(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$ są *równe* wtedy i tylko wtedy, gdy $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$.

Bardzo ważną jest rzeczą, by **nie utożsamiać wielomianu z funkcją wielomianową:** wielomianowi $P(x)$ możemy przypisać *funkcję wielomianową* $P\colon F \to F$, przyporządkowującą każdemu elementowi x ciała F element $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ ciała F.

Gdy $F = \mathbb{Q}$, lub $F = \mathbb{R}$, lub $F = \mathbb{C}$, różnym wielomianom odpowiadają różne funkcje wielomianowe (dlatego na kursie z Analizy Matematycznej zwykle nie rozróżnia sie pojęcia wielomianu i funkcji wielomianowej).

Jednakże sytuacja jest inna w przypadku ciał skończonych. Istotnie, rozważmy dwa wielomiany, $P(x) = x^2 + x$ i wielomian zerowy, nad ciałem $\mathbb{Z}_2$. Łatwo widać, że $P(0) = 0 \cdot 0 + 0 = 0 + 0 = 0$ i $P(0) = 1 \cdot 1 + 1 = 1 + 1 = 0$, czyli wielomianowi $P(x)$ odpowiada ta sama funkcja wielomianowa, co wielomianowi zerowemu.

Niech

$$P(x) = \sum_{i=0}^{n} a_i x^i, \quad Q(x) = \sum_{i=0}^{m} b_i x^i$$

będą wielomianami nad ciałem F. *Sumę* wielomianów $P(x)$ i $Q(x)$ definiujemy wzorem

$$P(x) + Q(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i)x^i,$$

a ich *iloczyn* wzorem

$$P(x) \cdot Q(x) = \sum_{k=0}^{m+n} c_k x^k, \quad \text{gdzie } c_k = \sum_{i+j=k} a_i b_j.$$

Dla dowolnych wielomianów z $F[x]$ zachodzą następujące własności:

- $(P_1(x) + P_2(x)) + P_3(x) = P_1(x) + (P_2(x) + P_3(x))$ (dodawanie wielomianów jest *łączne*);
- $P_1(x) + P_2(x) = P_2(x) + P_1(x)$ (dodawanie wielomianów jest *przemienne*);
- $(P_1(x) \cdot P_2(x)) \cdot P_3(x) = P_1(x) \cdot (P_2(x) \cdot P_3(x))$ (mnożenie wielomianów jest *łączne*);
- $P_1(x) \cdot P_2(x) = P_2(x) \cdot P_1(x)$ (mnożenie wielomianów jest *przemienne*);
- $(P_1(x) + P_2(x)) \cdot P_3(x) = (P_1(x) \cdot P_3(x)) + (P_2(x) \cdot P_3(x))$ (mnożenie wielomianów jest *rozdzielne* względem dodawania);
- $0 + P(x) = P(x) + 0 = P(x)$ (wielomian zerowy jest *elementem neutralnym* dla dodawania);
- $1 \cdot P(x) = P(x) \cdot 1 = P(x)$ (wielomian stały równy 1 jest *elementem neutralnym* dla mnożenia);
- iloczyn wielomianów niezerowych jest wielomianem niezerowym.

Dalej, mamy

$$\begin{aligned} \operatorname{st}(P_1(x) + P_2(x)) &\leqslant \max(\operatorname{st} P_1(x), \operatorname{st} P_2(x)), \\ \operatorname{st}(P_1(x) \cdot P_2(x)) &= \operatorname{st} P_1(x) + \operatorname{st} P_2(x). \end{aligned}$$

Twierdzenie 2 (Dzielenie wielomianów z resztą)**.** *Niech $P(x), Q(x) \in F[x]$. Jeśli $Q(x)$ nie jest wielomianem zerowym, to istnieją jednoznacznie wyznaczone wielomiany $M(x), R(x) \in F[x]$, $\operatorname{st} R(x) < \operatorname{st} Q(x)$, takie, że*

$$P(x) = M(x) \cdot Q(x) + R(x).$$

W powyższym twierdzeniu, $P(x)$ nazywamy *dzielną*, $Q(x)$ nazywamy *dzielnikiem*, $M(x)$ nazywamy *ilorazem* wielomianu $P(x)$ przez wielomian $Q(x)$, zaś $R(x)$ nazywamy *resztą* z dzielenia wielomianu $P(x)$ przez wielomian $Q(x)$

Jeśli dla wielomianów $P(x)$, $Q(x)$, reszta $R(x)$ z dzielenia $P(x)$ przez $Q(x)$ jest wielomianem zerowym, to mówimy, że wielomian $Q(x)$ *dzieli* wielomian $P(x)$ (lub wielomian $Q(x)$ jest *czynnikiem* wielomianu $P(x)$, lub że wielomian $P(x)$ jest *podzielny* przez $Q(x)$), i zapisujemy to $Q(x)|P(x)$.

Definicja. Element a ciała F nazywamy *pierwiastkiem* wielomianu $P(x) \in F[x]$, gdy $P(a) = 0$.

Twierdzenie 3 (Twierdzenie o reszcie)**.** *Reszta z dzielenia wielomianu $P(x) \in F[x]$ przez jednomian $(x - a)$, gdzie $a \in F$, jest równa $P(a)$.*

Twierdzenie 4 (Twierdzenie Bézout)**.** *$a \in F$ jest pierwiastkiem wielomianu $P(x) \in F[x]$ wtedy i tylko wtedy, gdy $(x - a)|P(x)$.*

Twierdzenie 5. *Wielomian $P(x) \in F[x]$ stopnia n ma co najwyżej n pierwiastków.*

Dowolny wielomian stopnia 1 ma dokładnie jeden pierwiastek. Istotnie, pierwiastkiem wielomianu $P(x) = a_0 + a_1 x$, gdzie $a_1 \neq 0$, jest a_0/a_1. Z powyższego twierdzenia wynika, że jest to jedyny pierwiastek.

Przykład. Wielomian $P(x) \in \mathbb{Z}_2[x]$, $P(x) = x^2 + x + 1$, nie ma pierwiastków.

Definicja. Mówimy, że wielomian $P(x) \in F[x]$ stopnia dodatniego jest *rozkładalny*, gdy istnieją takie wielomiany stopnia dodatniego $P_1(x), P_2(x) \in F[x]$, że $P(x) = P_1(x) \cdot P_2(x)$. Wielomian stopnia dodatniego, który nie jest rozkładalny, nazywamy *nierozkładalnym*.

Fakt 6. *Wielomian $P(x) \in F[x]$ stopnia 2 lub 3 jest nierozkładalny wtedy i tylko wtedy, gdy nie ma pierwiastków.*

Dowód. Jeśli wielomian stopnia co najmniej 2 ma pierwiastek, to, na podstawie twierdzenia Bézout, jest rozkładalny. Załóżmy teraz, że wielomian $P(x) \in F[x]$ stopnia 2 lub 3 jest rozkładalny. Zatem można go zapisać w postaci $P(x) = P_1(x) \cdot P_2(x)$, gdzie $1 \leqslant \operatorname{st} P_1(x) < \operatorname{st} P(x)$, $1 \leqslant \operatorname{st} P_2(x) < \operatorname{st} P(x)$. Ponieważ $\operatorname{st} P(x) = \operatorname{st} P_1(x) + \operatorname{st} P_2(x)$, co najmniej jeden z wielomianów $P_1(x)$, $P_2(x)$, musi być stopnia jeden. Znów z twierdzenia Bézout wnioskujemy, że $P(x)$ ma pierwiastek. □

Twierdzenie 7 (Jednoznaczność rozkładu na wielomiany nierozkładalne)**.** *Każdy wielomian stopnia dodatniego $P(x) \in F[x]$ jest iloczynem skończenie wielu wielomianów nierozkładalnych. Wielomiany nierozkładalne są wyznaczone jednoznacznie z dokładnością do kolejności czynników i mnożenia przez niezerowe elementy ciała F.*

Ostanie zdanie powyższego twierdzenia może być zilustrowane przez następujący przykład: w rozkładzie wielomianu $P(x) = x^2 + x \in \mathbb{R}[x]$ jako $P(x) = P_1(x) \cdot P_2(x)$, można wziąć $P_1(x) = x$, $P_2(x) = x + 1$, ale można też wziąć $P_1(x) = -\frac{1}{2}x - \frac{1}{2}$, $P_2(x) = -2x$ (formalnie są to różne rozkłady).

Przykład. Zbadajmy rozkładalność wszystkich wielomianów stopnia 2 z $\mathbb{Z}_2[x]$. Wielomian x^2 jest, oczywiście, rozkładalny. Wielomian $x^2 + 1$ jest też rozkładalny, ponieważ $x^2 + 1 = (x + 1)^2$. Wielomian $x^2 + x + 1$ jest nierozkładalny, gdyż nie ma pierwiastków (patrz Fakt 6). Wielomian $x^2+x = x(x + 1)$ jest rozkładalny.

Przykład. Zbadajmy (nie)rozkładalność wielomianu $x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$. Ponieważ nie ma on pierwiastków, w jego (ewentualnym) rozkładzie mogą wystąpić tylko nierozkładalne czynniki $P_1(x)$, $P_2(x)$ stopnia drugiego. Z poprzedniego przykładu wynika, że jedynym nierozkładalnym wielomianem stopnia drugiego jest x^2+x+1. Sprawdzamy teraz, że $x^4+x^2+1 = (x^2+x+1)^2$.

Przykład. Rozważmy teraz wielomian $x^4+x+1 \in \mathbb{Z}_2[x]$. Ponieważ nie ma on pierwiastków, powtarzając rozumowanie z powyższego przykładu dochodzimy do wniosku, że jedyny możliwy jego rozkład to $x^4+x+1 = (x^2+x+1)^2$, co jest fałszem. Jest to zatem wielomian nierozkładalny.