Wykład 6.

6.1 Nieco inaczej o wielomianach

Pojęcie wielomianu (jednej zmiennej, nad ciałem F) zwykle kojarzy się ze wzorem

$$\sum_{i=0}^{n} a_i \cdot x^i, \tag{6}$$

gdzie $a_0, \ldots, a_n$ są elementami ciała F, i może być definiowane na różne sposoby. Często wielomiany definiujemy jako funkcje $w : F \to F$ przyporządkowujące elementowi $a \in F$ wartość daną wzorem

$$w(a) = \sum_{i=0}^{n} a_i \cdot a^i.$$

Algebraicy rozważają także tzw. wielomiany formalne. Możemy definiować je jako wzory postaci (6), albo – równoważnie – jako ciągi $a_0, \ldots, a_n$ elementów ciała F, lub słowa $a_0 \ldots a_n$. Definicja powinna jednak utożsamiać wielomiany różniące się nieznaczącymi zerami, np. wielomiany opisane ciągami $a_0, \ldots, a_n$ oraz $a_0, \ldots, a_n, 0$. Jedna z precyzyjnych definicji wielomianów formalnych stwierdza, że są to nieskończone ciągi elementów ciała F, o wyrazach od pewnego miejsca stale równych 0. Taki ciąg $a_0, a_1, a_2, \ldots$ utożsamiamy ze wzorem

$$\sum_{i=0}^{\infty} a_i x^i \tag{7}$$

lub z wzorem

$$\sum_{i=0}^{n} a_i x^i,$$

jeżeli wiemy, że $a_i = 0$ dla wszystkich $i > n$.

Rozważmy przyporządkowanie, które wielomianowi formalnemu (7) przyporządkowuje wielomian w, czyli funkcję przekształcającą F w F i przyporządkowującą elementowi $a \in F$ wartość

$$w(a) = \sum_{i=0}^{\infty} a_i \cdot a^i.$$

Jeżeli F jest ciałem liczb rzeczywistych, to każdy wielomian $w : F \to F$ jednoznacznie wyznacza współczynniki z wzoru (7). Fakt ten można również wyrazić stwierdzając, że rozważane przyporządkowanie jest różnowartościowe. Inaczej jest w przypadku ciał skończonych: istotnie różne wielomiany formalne mogą wyznaczać tę samą funkcję. Tak jest np. dla wielomianów $1 + x + x^2$ i $1 + x^2 + x^4$ nad ciałem Z_2.

Zauważmy także, że dotychczas wielomiany utożsamialiśmy z ciągami ich wartości. Teraz będziemy utożsamiać wielomiany z ciągami współczynników.

Liczbę n nazywamy stopniem wielomianu $a_0, a_1, a_2, \ldots$, czyli wielomianu (7), jeżeli $a_n \neq 0$ oraz $a_i = 0$ dla wszystkich $i > n$. Zbiór wszystkich wielomianów formalnych zmiennej x nad ciałem F oznaczamy symbolem $F[x]$, a zbiór takich wielomianów stopnia $\leqslant n$ – symbolem $F^n[x]$. Nietrudno zauważyć, że zbiór $F^n[x]$ można utożsamiać ze zbiorem F^{n+1}.

Wielomiany dodajemy, mnożymy przez stałe (przez elementy ciała) i przez siebie. Dodawanie i mnożenie przez stałe wykonujemy w ten sposób, że wykonujemy odpowiednie operacje na współczynnikach. Jest oczywiste, że naturalna odpowiedniość między wielomianami stopnia $\leqslant n$ postaci (7) i ciągami $a_0, \ldots, a_n$ wyznacza izomorfizm przestrzeni liniowej F^{n+1} i zbioru $F^n[x]$ z dodawaniem i mnożeniem przez stałe z F.

Wielomiany formalne mnożymy zgodnie ze wzorem

$$(\sum_{i=0}^{\infty} a_i \cdot x^i) \cdot (\sum_{i=0}^{\infty} b_i \cdot x^i) = \sum_{i=0}^{\infty}(\sum_{j=0}^{i} a_j \cdot b_{i-j}) \cdot x^i.$$

Po uwzględnieniu, że wszystkie wyrazy – z wyjątkiem skończonej liczby – wielomianów $a_0, a_1, a_2, \ldots$ i $b_0, b_1, b_2, \ldots$ są równe 0, wzór ten (dla odpowiednich n i m) przyjmuje postać

$$(\sum_{i=0}^{n} a_i \cdot x^i) \cdot (\sum_{i=0}^{m} b_i \cdot x^i) = \sum_{i=0}^{n+m}(\sum_{j=\max(0,i-m)}^{\min(n,i)} a_j \cdot b_{i-j}) \cdot x^i.$$

Aby się o tym przekonać zauważmy, że w i-tym współczynniku iloczynu indeksy wyrazów b_{i-j} spełniają nierówność $0 \leqslant i - j \leqslant m$, czyli $i - m \leqslant j \leqslant i$, a indeksy wyrazów a_j – nierówność $0 \leqslant j \leqslant n$. Łącząc te nierówności mamy, że $\max(0, i - m) \leqslant j \leqslant \min(n, i)$. Z tego wzoru wynika w szczególności, że mnożąc wielomiany stopni n i m otrzymujemy wielomian stopnia $n + m$.

Zbiór $F[x]$ jest zamknięty ze względu na mnożenie i z dodawaniem oraz mnożeniem wielomianów tworzy pierścień. Zbiory $F^n[x]$ nie są zamknięte ze względu na mnożenie. Łatwo jednak zauważyć, że jeżeli mnożymy dwa wielomiany ze zbioru $F^n[x]$, stopnia k i l odpowiednio, to ich iloczyn należy do $F^n[x]$ wtedy i tylko wtedy, gdy $k + l \leqslant n$.

W dalszym ciągu będziemy zajmować się wielomianami formalnymi, ale będziemy opuszczać przymiotnik „formalny".

6.2 Kody cykliczne

Liniowy kod $K \subseteq F^{n+1}$ będziemy nazywać cyklicznym, jeżeli dla dowolnego ciągu $(a_0, \ldots, a_n) \in K$ do kodu K należy także ciąg $(a_n, a_0, \ldots, a_{n-1})$.

Lemat 6.1 *Niech $K \subseteq F^n[x]$ będzie kodem cyklicznym. Jeżeli $g \in K$ jest wielomianem stopnia k, to iloczyny $g(x)$, $xg(x)$, $x^2g(x)$, $\ldots$, $x^{n-k}g(x)$ należą do K.*

Dowód. Oczywiście, jeżeli $a_0, \ldots, a_n$ jest ciągiem współczynników wielomianu $g = g(x)$ oraz $s \leqslant n-k$, to $0, \ldots, 0, a_0, \ldots, a_n$ jest ciągiem (ciąg ten rozpoczyna się s zerami) współczynników wielomianu $x^s \cdot g(x)$. Ponieważ wielomian g jest stopnia k, więc $a_i = 0$ dla $i > n - s \geqslant k$. Wobec tego, ciągiem współczynników wielomianu $x^s \cdot g(x)$ jest też $0, \ldots, 0, a_0, \ldots, a_{n-s}$. Z tego samego powodu, ten ostatni ciąg otrzymujemy s-krotnie przestawiając ostatni wyraz ciągu $a_0, \ldots, a_n$ na początek. Wobec cykliczności kodu K oznacza to, że $x^s \cdot g(x) \in K$. □

Jeżeli K jest kodem cyklicznym, to generatorem K nazywamy niezerowy wielomian $g \in K$ minimalnego stopnia, ze współczynnikiem przy najwyższej potędze równym 1. Oczywiście, każdy kod cykliczny różny od $\{\vec{0}\}$ ma generator.

Wniosek 6.2 *Jeżeli $K \subseteq F^n[x]$ jest kodem cyklicznym z generatorem g stopnia k, to*

$$K = \{p \cdot g : p \in F^n[x] \wedge p \text{ jest wielomianem stopnia } \leqslant n-k\}.$$

Dowód. Podany zbiór jest zawarty w K na mocy liniowości K i lematu 6.1. Aby dowieść drugie zawieranie weźmy wielomian $w \in K$ i podzielmy go przez g. Mamy więc $w(x) = p(x) \cdot g(x) + r(x)$ dla pewnych wielomianów p i r stopnia odpowiednio $\leqslant n-k$ i $< k$. Wobec tego, $r(x) = w(x) - p(x) \cdot g(x) \in K$ i jest stopnia mniejszego niż generator g. Oznacza to, że wielomian r jest równy 0 i, w konsekwencji, $w(x) = p(x) \cdot g(x)$ dla pewnego wielomianu p stopnia $\leqslant n-k$. □

Wniosek 6.3 *Jeżeli $K \subseteq F^n[x]$ jest kodem cyklicznym z generatorem g stopnia k, to wielomiany $g(x)$, $x \cdot g(x)$, $\ldots$, $x^{n-k} \cdot g(x)$ tworzą bazę przestrzeni K. Tak więc K jest przestrzenią wymiaru $n-k+1$.*

Dowód. Niech $g \in K$ będzie generatorem kodu. Jest oczywiste, że dla $i \leqslant n-k$ wielomian $x^i \cdot g(x) \in K$ i ciąg współczynników tego wielomianu zaczyna się i zerami. Stąd natychmiast otrzymujemy, że dla $i \leqslant n-k$ wielomiany $x^i \cdot g(x)$ tworzą liniowo niezależny podzbiór K. Z wniosku 6.2 wynika, że także generują K. □

Wniosek 6.4 *Generator kodu cyklicznego $K \subseteq F^n[x]$ jest wyznaczony jednoznacznie.*

Twierdzenie 6.5 *Wielomian g jest generatorem pewnego kodu cyklicznego zawartego w $F^n[x]$ wtedy i tylko wtedy, gdy jest dzielnikiem stopnia $\leqslant n$ wielomianu $x^{n+1} - 1$ i ma współczynnik 1 przy najwyższej potędze.*

Dowód. Najpierw zauważmy, że jeżeli w jest wielomianem o współczynnikach $a_0, \ldots, a_n$, to $a_n, a_0, \ldots, a_{n-1}$ jest ciągiem współczynników wielomianu w' danego wzorem

$$w'(x) = x \cdot w(x) - a_n \cdot (x^{n+1} - 1). \tag{8}$$

Wobec tego, dla dowolnego kodu cyklicznego K warunek $w \in K$ implikuje, że $w' \in K$. Ponadto, dowolny kod liniowy K spełniający podaną implikację jest cykliczny.

Przypuśćmy, że g jest wielomianem stopnia k generującym kod cykliczny $K \subseteq F^n[x]$. Podzielmy wielomian $x^{n+1} - 1$ przez g. Mamy więc

$$x^{n+1} - 1 = p(x) \cdot g(x) + r(x)$$

dla pewnego wielomianu p stopnia $n-k+1$ i pewnego wielomianu r stopnia $< k$. Niech $w(x) = x^{n-k} \cdot g(x)$. Oczywiście, w jest wielomianem stopnia n należącym do K. Niech w' będzie zdefiniowany wzorem (8). Mamy więc, że $w' \in K$. Zauważmy, że

$$w'(x) = x^{n-k+1} \cdot g(x) - p(x) \cdot g(x) + r(x) = (x^{n-k+1} - p(x)) \cdot g(x) + r(x).$$

Współczynnik wielomianu p przy potędze x^{n-k+1} jest równy 1. Wobec tego, wielomian $x^{n-k+1} - p(x)$ ma stopień $\leqslant n-k$. Z wniosku 6.2 wynika, że $(x^{n-k+1} - p(x)) \cdot g(x) \in K$ i, w konsekwencji,

$r \in K$. Ponieważ r ma stopień mniejszy od generatora kodu, więc $r = 0$. Oznacza to, że g jest dzielnikiem $x^{n+1} - 1$.

Przypuśćmy, że g jest dzielnikiem $x^{n+1} - 1$ stopnia $k \leqslant n$ ze współczynnikiem 1 przy najwyższej potędze. Niech

$$K = \{p \cdot g \in F^n[x] : p \in F^n[x] \text{ i ma stopień } \leqslant n - k\}.$$

Oczywiście, K jest kodem liniowym. Udowodnimy, że K jest kodem cyklicznym. Stąd oczywiście wyniknie, że g jest generatorem kodu K.

Weźmy wielomian p stopnia $\leqslant n - k$ ze współczynnikiem a przy potędze x^{n-k} i rozważmy – zgodnie ze wzorem (8) dla $w(x) = p(x) \cdot g(x)$ – wielomian

$$w'(x) = x \cdot p(x) \cdot g(x) - a \cdot (x^{n+1} - 1).$$

Aby dowieść cykliczność kodu K, wystarczy wykazać, że $w' \in K$. Przedstawmy więc $x^{n+1} - 1$ jako iloczyn $q(x) \cdot g(x)$ dla pewnego wielomianu q stopnia $n + 1 - k$. Współczynnik przy najwyższej potędze wielomianu q jest równy 1. Zauważmy, że

$$w'(x) = x \cdot p(x) \cdot g(x) - a \cdot q(x) \cdot g(x) = (x \cdot p(x) - a \cdot q(x)) \cdot g(x).$$

Własność $w' \in K$ wynika stąd, że wielomian $x \cdot p(x) - a \cdot q(x)$ jest stopnia $\leqslant n - k$. Sprawdzamy to osobno dla przypadku $a = 0$ i dla jego zaprzeczenia. $\square$