Algebra ISIM 2. Wykład 12: Bazy Groebnera

"Pierścień wielomianów" będzie oznaczać pierścień $K[X_1, \ldots, X_n]$; skrótowo będziemy go zapisywać jako $K[X]$ i używać multiindeksów $\alpha \in \mathbf{N}^n$ ($0 \in \mathbf{N}$).

Aby określić stopień wielomianu wielu zmiennych potrzebujemy porządku na zbiorze multiindeksów. *Porządek jednomianowy* na zbiorze $\mathbf{N}^n$ to dobry porządek spełniający warunek: $\alpha > \beta \Rightarrow (\alpha + \gamma > \beta + \gamma)$. Przykłady:

- lex: $\alpha > \beta \iff$ pierwszy niezerowy wyraz $\alpha - \beta$ jest dodatni;
- grlex: $\alpha > \beta \iff |\alpha| > |\beta|$ lub $|\alpha| = |\beta|$ i pierwszy niezerowy wyraz $\alpha - \beta$ jest dodatni;
- grevlex: $\alpha > \beta \iff |\alpha| > |\beta|$ lub $|\alpha| = |\beta|$ i ostatni niezerowy wyraz $\alpha - \beta$ jest ujemny.

Przy ustalonym porządku jednomianowym określamy *stopień* i *wyraz wiodący* złożony z *współczynnika wiodącego* i *jednomianu wiodącego.*

Dzielenie z resztą.

Przy ustalonym porządku wielomianowym można wykonać dzielenie z resztą wielomianu f przez ciąg wielomianów $F = (f_1, \ldots, f_k)$. Bierzemy wyraz wiodący f i sprawdzamy, czy dzieli się on przez wyrazy wiodące kolejnych f_i. Jeśli tak, to pierwszego pasującego f_i używamy do skasowania tego wyrazu wiodącego; jeśli nie, to wyraz wiodący odejmujemy od f i dodajemy do reszty R. Powtarzamy tę procedurę aż do wyzerowania f. Ostateczną wartość R nazywamy *resztą* f modulo F, i oznaczamy $\overline{f}^F$ lub $f \bmod F$.

Przykład (lex). Niech $f = xy^2 - x$, $F = (xy + 1, y^2 - 1)$. Wtedy $f \bmod F = -x - y$. Jeśli jednak zamienić kolejność wyrazów F, to dostajemy resztę 0; oznacza to, że f należy do ideału generowanego przez F, mimo że $f \bmod F \neq 0$. Jest to oczywiście sytuacja bardzo niepożądana.

Bazy Groebnera.

Skończony podzbiór G ideału $I \lhd K[X]$ nazywamy *bazą Groebnera* tego ideału, jeśli wyrazy wiodące elementów G generują ten sam ideał pierścienia $K[X]$, co wyrazy wiodące wszystkich elementów I.

Z noetherowskości $K[X]$ wynika, że każdy ideał ma bazy Groebnera. Reszta z dzielenia elementu I przez bazę Groebnera I wynosi 0; wynika stąd, że baza Groebnera ideału generuje ten ideał. Okazuje się, że reszta z dzielenia dowolnego wielomianu f przez bazę Groebnera pewnego ideału I nie zależy od kolejności elementów bazy, a zerowanie się tej reszty jest równoważne należeniu f do I. Wynika to z następującego faktu charakteryzującego resztę.

Fakt. *Niech $f \in K[X]$ i niech G będzie bazą Groebnera ideału $I \lhd K[X]$. Istnieje wtedy jedyne $r \in K[X]$, takie że*

1) $f = g + r$ dla pewnego $g \in I$;
2) żaden wyraz r nie dzieli się przez żaden wyraz wiodący żadnego elementu G.

Dowód. Istnienia dostarcza opisany wyżej algorytm dzielenia z resztą. Jednoznaczność: z 1) widzimy, że różnica dwóch wersji r należy do I, zatem jej wyraz wiodący dzieli się przez wyraz wiodący pewnego elementu G; to jednak przeczy warunkowi 2).

Algorytm Buchbergera.

Jest to procedura przerabiająca układ generatorów ideału na jego bazę Groebnera. Używa ona pojęcia *S-wielomianu,* który określamy – dla $f, g \in K[X]$ – jako

$$S(f,g) = \frac{X^\gamma}{LT(f)} f - \frac{X^\gamma}{LT(g)} g,$$

gdzie X^γ to najmniejsza wspólna wielokrotność wyrazów wiodących $LT(f), LT(g)$ wielomianów f, g. Innymi słowy, kasujemy wyrazy wiodące wielomianów f, g, domnażając przedtem tak, by przyjęły wspólny stopień.

Tw. *Niech G, F będą skończonymi podzbiorami $K[X]$.*

K) (Kryterium Buchbergera) G jest bazą Groebnera ideału $I = (G) \iff (\forall g, g' \in G)(S(g,g') \bmod G = 0)$.
A) (Algorytm Buchbergera) Niech $I = (F)$. Dla każdej pary $f, f' \in F$ policzmy $S(f,f') \bmod F$; otrzymane niezerowe reszty dołączmy do F. Powtarzanie tej procedury w skończenie wielu krokach prowadzi do bazy Groebnera I.

Przykład. Bazą Groebnera ideału $(xy + 1, y^2 - 1)$ jest $G = (xy + 1, y^2 - 1, x + y)$.

Lemat. *Jeśli wielomiany $f_i \in K[X]$ są stopnia δ, zaś stopień $\sum_i a_i f_i$ jest $< \delta$ (dla pewnych $a_i \in K$), to $\sum_i a_i f_i = \sum_{i,j} a_{ij} S(f_i, f_j)$ (dla pewnych $a_{ij} \in K$).*

Istotnie, można założyć $LT(f_i) = X^\delta$; wtedy $S(f_i, f_j) = f_i - f_j$. Mamy też wówczas $\sum_i a_i = 0$, a zatem $\sum_i a_i f_i$ jest kombinacją różnic $f_i - f_{i+1}$.

Dowód tw. K)

($\Leftarrow$) Wynika wprost z $S(g, g') \in I$.

($\Rightarrow$) Niech $G = (g_1, \ldots, g_k)$ i niech $f \in I = (G)$. Wtedy f da się przedstawić w postaci $f = \sum_i h_i g_i$; pokażemy, że istnieje takie przedstawienie dodatkowo spełniające $\delta := \max_i \deg(h_i g_i) = \deg(f)$. (Ten dodatkowy warunek wymusza już $LT(g_i) | LT(f)$ dla pewnego g_i, co daje tezę.) Jeśli $\delta > \deg(f)$, to wyrazy stopnia δ w $\sum_i h_i g_i$ sumują się do zera. Można więc zastosować lemat do tych $f_i = LT(h_i) g_i$, które są stopnia δ. Dla takich i, j:

(1) $S(LT(h_i)g_i, LT(h_j)g_j) = X^\gamma S(g_i, g_j)$ i ma stopień $< \delta$ (dla pewnego γ zależnego od i, j);

(2) $S(g_i, g_j) = \sum_s w_{ijs} g_s$, gdzie składniki są stopnia $\leq \deg S(g_i, g_j)$ (z warunku $S(g_i, g_j) \bmod G = 0$).

Lemat pozwala więc zastąpić wyrażenie $\sum_i h_i g_i$ wyrażeniem tej samej postaci, ale o składnikach stopnia $< \delta$. Iterując opisaną procedurę dostajemy ostatecznie $\delta = \deg f$.

A) Każdy krok algorytmu powiększa ideał generowany przez wyrazy wiodące elementów F. Ale $K[X]$ jest noetherowski, więc algorytm zatrzymuje się.