Базисы Грёбнера.

Пусть F это произвольное поле, и пусть R = F[x1,...,xn] обозначает кольцо полиномов от m переменных x1,...,xm. Непустое подмножество I множества R называется идеалом, если

1. для a, b из I: a+b принадлежит I
2. для a из I: ab принадлежит I для любого b из R.

Любой набор полиномов f1,..., fn из R порождает идеал в R естественным образом, а именно, это множество всех полиномов вида: h1f1 + ... + hnfn, где hi это произвольные элементы R. это идеал обозначается <f1,...,fn>. Для идеала I кольца R, если I = <f1,...,fn>, тогда мы говорим, что I порожден f1,...,fn или, что множество {f1,...,fn} это базис в I. Идеал может иметь несколько базисов, и разные базисы могут содержать разное число элементов. Также элементы базиса в идеале не обязательно линейно независимы над F, но могут быть легко приведены к линейно независимым. Теорема Гильберта о базисе гарантирует то, что любой идеал I в R может быть порожден конечным числом полиномов.

Идеал I = <f1,...,fn> точно фиксирует общие нули полиномов f1,...,fn в том смысле, что:

1. любой общий ноль f1,...,fn является нулем каждого g из I;
2. если у I есть другой базис, например I = <g1,...,gn>, тогда точка в F^m является общим нулем f1,...,fn тогда и только тогда, когда она общий ноль g1,...,gn.

Базис Грёбнера для идеала I из R это некоторый «удобный» базис в I, который предоставляет нам лучше «контролировать» общие нули идеала и производить вычисления, связанные с идеалом (например, проверять принадлежит ли данный полином g из R к I). В качестве простого примера рассмотрим два полинома f1, f2 из F[x] (полиномы одной переменной) м идеал I = <f1, f2> в F[x]. Пусть d(x) = gcd(f1(x),f2(x)). Тогда мы имеем I = <d(x)>. Таким образом, d(x) сам является базисом идеала, и он удобен в том смысле, что степень d(x) совпадает с числом общих нулей f1(x) и f2(x) (в алгебраическом замыкании F) и полином g(x) из F[x] принадлежит I в том и только том случае, если g(x) делится на d(x). Для полиномов нескольких переменных базис Грёбнера предоставляет аналогичную информацию и даже намного больше. Чтобы точно определить базис Грёбнера, нам сперва потребуется ввести порядки на мономах.

2.1 Мономиальные порядки.

Мы используем следующие обозначения. Пусть N = {0,1,2,...}, $Z=\{0,\pm1,\pm2,\dots\}$ и R множество вещественных чисел .Для $\alpha=(\alpha_1,\dots,\alpha_m)\in N$

$$x^\alpha = x_1^{\alpha_1}\dots x_m^{\alpha_m}$$

называется мономом в F[x1,...,xm]. Таким образом, имеется взаимно-однозначное соответствие между мономами в F[x1,...,xm] и элементами N^m.

Мономиальный порядок на F[x1,...,xm] это любой полный порядок > на всех мономах такой что:

1. $x^\alpha > 1$ для любого $\alpha\in N^m$, где $\alpha\neq 0$;
2. если $x^\alpha > x^\beta$, то $x^\alpha\cdot x^\gamma > x^\beta\cdot x^\gamma$ для всех $\gamma\in N^m$.

Под «полным порядком» выше мы понимаем то, что любые два монома могут быть сравнены; это значит, что они либо равны, либо один больше другого. Второе условие влечет то, что при умножении полинома на моном упорядочение его членов не изменится. Это свойство важно для длинного деления полиномов. Также эти два условия гарантируют, что если x^α делится на x^β, то $x^\alpha \geqslant x^\beta$.