УДК 512 624: 003.26

Поля и многочлены, элементы полей как корни полиномов

Королёва М.Н., Липницкий В.А.
Белорусский национальный технический университет
Военная академия Республики Беларусь

Поля относятся к разряду важнейших объектов современной алгебры, элементы которых сочетают в себе и аддитивные, и мультипликативные аспекты. Один из них – характеристика поля. По определению, это аддитивный порядок мультипликативной единицы поля. По значениям характеристики все семейство полей разбивается на бесконечное множество непересекающихся классов. Все поля каждого отдельного класса имеют единственное общее минимальное подполе F – поле классов вычетов Z/pZ по простому модулю p или же поле рациональных чисел Q и являются векторными пространствами над этим минимальным подполем.

Если конкретное поле P имеет конечную размерность n над минимальным подполем, то степени $1, \beta, \beta^2, ..., \beta^i$ произвольного элемента $\beta \in P$ образуют линейно зависимую над F систему векторов. Коэффициенты равной нулю линейной комбинации названных векторов определяют полином $f(x)$ с корнем β. Разложение $f(x)$ на неприводимые множители определяет неприводимый полином $p(\mathrm{x})$ с корнем β (минимальный полином элемента β).

Поэтому β называют алгебраическим над полем F. Задачу распределения элементов поля Галуа по их минимальным полиномам можно решить двояко. Если β – один из корней неприводимого полинома, то остальными будут элементы $\beta^p, \beta^{p^2}, ..., \beta^{p^\nu}$ для $\nu = i$ или же делящего i.

Тогда $p(\mathrm{x}) = (x-\beta)\cdot(x-\beta^p)\cdot...\cdot(\mathrm{x}-\beta^{p^\nu})$.

Для получения явных коэффициентов этого полинома из поля F надо раскрыть скобки или же воспользоваться формулами Виета. Всякое конечное поле $GF(p^n)$ единственно, нормально и сепарабельно над полем $F = Z/pZ$.

Поэтому все корни каждого неприводимого над Z/pZ полинома $p(\mathrm{x})$ степени n находятся в этом поле. Отсюда следует методика определения числа всех неприводимых полиномов $p(\mathrm{x})$ степени n.