

Алгебраическая теория чисел (часть 1)

Александр Сивацкий

1 Содержание

В первой части курса изучаются кольца целых алгебраических чисел в конечных расширениях поля $\mathbb{Q}$. Такие кольца являются аналогами кольца $\mathbb{Z}$ в поле $\mathbb{Q}$.

Пусть K – подполе поля $\mathbb{C}$, являющееся конечным расширением поля $\mathbb{Q}$. Элемент $x \in K$ называется целым алгебраическим числом, если он является корнем многочлена с целыми коэффициентами и со старшим коэффициентом 1. Мы показываем, что целые алгебраические числа поля K образуют дедекиндово кольцо (обозначаемое O_K), то есть область целостности, в которой для любых двух идеалов $I_1 \subset I_2$ существует идеал J такой, что $I_1 = I_2 J$. По определению дробный идеал – это множество aI , где $a \in K^*$, и $I \subset O_K$. Доказывается, что по отношению к операции умножения дробные идеалы образуют абелеву группу (обозначаемую $I(K)$). Факторгруппа $I(K)$ по подгруппе главных дробных идеалов называется группой классов идеалов $Cl(K)$. Мы показываем, что эта группа всегда конечна и вычисляем ее в некоторых случаях. Как следствие доказывается, что для любого идеала $I \subset O_K$ существует конечное расширение L/K , такое, что идеал $IO_L \subset O_L$ главный.

Мы определяем норму идеала, и вводим понятия дифференты и дискриминанта, необходимые для критерия ветвления идеалов. Для иллюстрации соответствующей техники рассматриваются квадратичные и круговые поля. Например, *большая теорема Ферма для $p = 3$* доказывается с использованием кольца целых алгебраических чисел $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ в $\mathbb{Q}(\sqrt{-3})$. Неожиданным образом, применяя круговые расширения, можно доказать частный случай *теоремы Дирихле об арифметической прогрессии*, а именно случай прогрессии $1, 1+n, 1+2n, \dots$. Еще одно применение круговых расширений – доказательство того что любая конечная абелева группа является группой Галуа некоторого расширения поля $\mathbb{Q}$.

В заключительных лекциях мы рассматриваем конечные поля $\mathbb{F}_q$, и исследуем многочлены от нескольких переменных над этими полями. В частности, показывается, что любой однородный многочлен f степени d от $d+1$ переменных над $\mathbb{F}_q$ имеет нетривиальный ноль, то есть существует вектор $0 \neq (a_1, \dots, a_{d+1}) \in \mathbb{F}_q^{d+1}$ такой что $f(a_1, \dots, a_{d+1}) = 0$. Также мы изучаем диагональные многочлены g over $\mathbb{F}_q$ и даем нижнюю и верхнюю оценки для числа решений уравнения $g = 0$.

В последней лекции рассматриваются p -адические поля $\mathbb{Q}_p$ и квадратичные формы над ними. Этот материал понадобится во второй части курса при доказательстве *теоремы Хассе-Минковского* о квадратичных формах над $\mathbb{Q}$.

2 Лекции

1. Кольцо целых алгебраических чисел O_K для конечного расширения поля $K/\mathbb{Q}$. Примеры.
2. Кольца дискретного нормирования. Дедекиндовы кольца. Кольца целых алгебраических чисел как дедекиндовы кольца.
3. Дробные идеалы. Разложение идеалов в произведение простых идеалов.
4. Следствия Китайской теоремы об остатках. Порождаемость идеалов в кольце O_K двумя элементами.
5. Норма идеала, индекс ветвления и степень инерции.
6. Дифферента и дискриминант. Критерий разветвленности простого идеала.
7. Круговые полиномы и поля. Частный случай теоремы Дирихле об арифметической прогрессии.
8. Кольцо целых алгебраических чисел кругового поля $\mathbb{Q}(\sqrt[p]{1})$ для простого p . Конечные абелевы группы как группы Галуа расширений поля $\mathbb{Q}$.
9. Теорема Куммера о разложении простых чисел в произведение простых идеалов. Примеры.
10. Конечность группы классов идеалов. Примеры.
11. Большая теорема Ферма для $p = 3$.
12. Мультипликативные характеры конечных полей. Суммы Гаусса. Квадратичные расширения $\mathbb{Q}$ как подполя круговых полей.

13. Суммы Якоби. Теорема о сумме двух квадратов.
14. Диагональные полиномы над конечными полями. C_1 свойство конечных полей.
15. p -адическое поле $\mathbb{Q}_p$. Квадратичные формы над $\mathbb{Q}_p$.

3 Пререквизиты

Для понимания курса достаточно знать основы линейной алгебры, теории полей и теории групп.