БФУ им. И. Канта – Методы алгебраической теории чисел в криптографии.
Е.Малыгина (2020 – Осенний семестр)

Лекция №1 (07.09.20)

---

1. Алгебраические числовые поля.

1.1. Расширения полей.

Пусть K и L – поля. Если K – подполе поля L, то будем говорить, что L – *расширение поля* K и обозначать L/K. Например, $\mathbb{C}/\mathbb{Q}$ и $\mathbb{C}/\mathbb{R}$ – расширения полей.

Определение 1. *Пусть L/K – расширение полей и $\alpha \in L$. Будем говорить, что α –* алгебраический над K, *если существует ненулевой многочлен $g \in K[X]$, такой, что $g(\alpha) = 0$.*

Предложение 1. *Пусть α – алгебраический над K. Тогда существует единственный многочлен $f \in K[X]$, такой, что $f(\alpha) = 0$ и f – неприводимый и унитарный многочлен. Будем называть этот многочлен f* минимальным многочленом *над K.*

Определение 2. *Пусть L/K – расширение. Будем говорить, что L/K –* алгебраическое, *если каждый $\alpha \in L$ является алгебраическим над K. Назовем расширение L/K конечным, если L имеет конечную размерность как K-векторное пространство.*

Если L/K – конечное расширение, то определим *степень* $[L : K]$ – размерность L как K-векторного пространства.

Предложение 2. *Пусть L/K – расширирение полей. Элемент $\alpha \in L$ является алгебраическим над K тогда и только тогда, когда существует конечное расширение поля K внутри L, которое содержит α.*

Следствие 1. *1. Элемент $\alpha \in L$ – алгебраический над K тогда и только тогда, когда степени α порождают конечномерное K-подпространство L.*

2. *Если α – алгебраический над L, то существует единственное наименьшее расширение поля K в L, которое содержит α, а именно, K-подпространство, порожденное тепенями α, и K-базис этого подпространства есть $1, \alpha, \cdots \alpha^{d-1}$, где d – степень минимального многочлена элемента α над K.*

Предложение 3. *Расширение M/K явлется конечным тогда и только тогда, когда L/K и M/L – оба конечны, и в этом случае*

$$[M : K] = [M : L][L : K].$$