Алгебра 3
25.09.97

Круговые поля

Часть 1. Многочлены над кольцами.

Теорема. Кольцо $\mathbb{Z}[x]$ факториально.

Доказать эту теорему аналогично кольцу $\mathbb{Q}[t]$ не удастся, так как это кольцо не является кольцом главных идеалов: идеал $(2, x)$ не главный. Поэтому придется поступить по-другому.

Содержанием многочлена $P \in \mathbb{Z}$ называется наибольший общий делитель его коэффициентов, обозначается СОД(P).

Лемма Гаусса. Если СОД$(P) =$ СОД$(Q) = 1$, то СОД$(PQ) = 1$.

Предположим, это не так и СОД$(PQ) \neq 1$. Тогда найдется простое p, такое, что $PQ \vdots p$. Обозначим через $\overline{H}$ образ H при естественном гомоморфизме $\mathbb{Z}[x] \to \mathbb{F}_p[x]$.

Тогда $\overline{PQ} = \overline{P} \cdot \overline{Q}$, но по предположению $\overline{PQ} = 0$, откуда либо $\overline{P} = 0$, либо $\overline{Q} = 0$. Противоречие.

Следствие. СОД$(PQ) =$ СОД(P) СОД(Q).

Пусть $R \in \mathbb{Q}[x]$. Тогда R можно представить в виде $\dfrac{a}{b}S$, где $S \in \mathbb{Z}[x]$, СОД$(S) = 1$, причем такое представление единственно с точностью до знака. Из Леммы следует, что эти представления перемножаются.

Значит, любому разложению многочлена над $\mathbb{Z}$ соответствуе его разложение на множители над $\mathbb{Q}$ (с выделением содержания), и наоборот. Поэтому основная теорема арифметики верна и в кольце $\mathbb{Z}[x]$. Доказательсто окончено.

Из доказательства следует, что если многочлен неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$ — важный критерий неприводимости.

Замечание. В доказательстве никак не использовались специальные свойства кольца $\mathbb{Z}$, и на самом деле доказана более общая теорема о том, что если кольцо A факториально, то $A[x]$ тоже. Из этого, например, следует, что кольцо $\mathbf{k}[t_1, t_2, \ldots, t_n]$ факториально.

Критерий Эйзенштейна. Пусть $P \in \mathbb{Z}[x]$, $P = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, СОД$(P) = 1$. Тогда если существует такое простое p, что 1) $p \not| a_n$, 2) $\forall i < n \quad p \mid a_i$, 3) $p^2 \not| a_0$, то P неприводим.

Если это не так, то пусть $P = QR$. Рассмотрим все по модулю p. Тогда

$$\begin{cases} \overline{P} = \overline{Q} \cdot \overline{R} \\ \overline{P} = a_nx^n. \end{cases}$$

Значит, без потери общности $\overline{Q} = a_nx^k$. Если $k = 0$ или $k = n$, то тогда степень одного из многочленов P и Q равна n, а тогда степень другого равна нулю даже над $\mathbb{Z}$, чего не может быть, поскольку СОД$(P) = 1$. Если же $0 < k < n$, то тогда $\overline{P}(0) = \overline{Q}(0) = 0 \Rightarrow a_0 \vdots p^2$. Противоречие. Значит, многочлен P неприводим.

Пример применения критерия Эйзенштейна: $\Phi_p = x^{p-1} + \ldots + x + 1$ неприводим (нужно сделать замену x на $y + 1$).

Часть 2. Круговые многочлены.

Примитивным (первообразным) корнем степени n из 1 называется комплексное число ζ, имеющее в группе всех корней n-ой степени из 1 порядок n. Количество примитивных корней степени n из 1 равняется функции Эйлера $\phi(n)$.

Определение. $\Phi_n(x) = \prod\limits_{\zeta \text{ примитивный } \sqrt[n]{1}} (x - \zeta), \quad \deg \Phi_n(x) = \phi(n).$

Утверждение. $x^n - 1 = \prod\limits_{d|n} \Phi_d(x).$

Следствие. $\Phi_n(x) \in \mathbb{Z}[x]$.

Это легко доказать по индукции.

ТЕОРЕМА. $\Phi_n(x)$ неприводим.

Доказательство.

Предположим, это не так. Пусть ζ — первообразный корень. Пусть $f(x)$ — неприводимый делитель Φ_n, такой что $f(\zeta) = 0$.

Предположим, нашлось простое $p \not| \, n$, такое что ζ^p не является корнем f. Пусть $g(x)$ — неприводимый делитель Φ_n, такой что $g(\zeta^p) = 0$. Тогда по основной теореме арифметики $\Phi_n(x) = f(x)g(x)R(x)$, а так как ζ — корень $g(x^p)$, то $g(x^p) \,\vdots\, f(x)$. Приведем все по модулю p.

$$\overline{g}(x^p) = [\overline{g}(x)]^p \,\vdots\, \overline{f}(x)$$

Пусть $\overline{h}(x)$ — какой-нибудь простой делитель $\overline{f}(x)$. Тогда

$$\begin{gathered}\overline{g}(x) \,\vdots\, \overline{f}(x) \\ \overline{\Phi}_n(x) \,\vdots\, \overline{h}^2(x) \\ x^n - 1 \,\vdots\, \overline{h}^2(x) \\ (x^n - 1)' \,\vdots\, \overline{h}(x)\end{gathered}$$

Противоречие — по предположению $p \not| \, n$ и $(x^n - 1)' = nx^n$ не имеет общих делителей с $x^n - 1$.

Итак, если $p \not| \, n$, а ζ — первообразный корень, то ζ^p — тоже первообразный корень — является корнем того же минимального многочлена, что и ζ. Если η — произвольный первообразный корень, то $\eta = \zeta^{p_1 \cdots p_k}$, где все простые p_i не делят n. Применяя предыдущее заключение k раз, получаем, что и η является корнем того же минимального многочлена $f(x)$, что и ζ. Таким образом, $\deg f(x) \geqslant \phi(n)$, откуда $f(x) = \Phi_n(x)$.

Доказательство окончено.

Часть 3. Автоморфизмы круговых полей

Если ζ —первообразный корень, то

$$\mathbb{Q}(\sqrt[n]{1}) = \mathbb{Q}(\zeta) = \mathbb{Q}[t]/(\Phi_n(t))$$

.

Если α — автоморфизм $\mathbb{Q}(\zeta)$ над $\mathbb{Q}$, то α полностью задается равенством

$$\alpha(\zeta) = \zeta^k, \qquad (n,k) = 1$$

Отсюда следует, что

$$\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*.$$

Замечание. $\{\, \zeta^k \mid (k,n) = 1 \,\}$ образует базис $\mathbb{Q}(\zeta)$ над $\mathbb{Q}$.

Рассмотрим теперь частный случай $n = p$ — простое число. Тогда

$$\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/(p-1)\mathbb{Z}$$

Значит, существует автоморфизм-образующая $\sigma(\zeta) = \zeta^g$, где g — образующая группы $(\mathbb{Z}/p\mathbb{Z})^*$.

Пример: $p = 17$, $g = 3$.

$$\begin{gathered} \sigma(\zeta) = \zeta^3 \\ \sigma^2(\zeta) = \zeta^9 \\ \vdots \\ \sigma^8(\zeta) = \zeta^{-1} \\ \vdots \end{gathered}$$

Все примитивные корни можно перенумеровать: $\zeta_i = \sigma^i(\zeta) = \zeta^{g^i}$.

Если ϕ — автоморфизм $\mathbb{Q}(\zeta)$ над $\mathbb{Q}$, то $\mathbb{Q}(\zeta)^\phi$ обозначает подполе его инвариантов.

Например, $\mathbb{Q}(\zeta)^\sigma = \mathbb{Q}$, в то время как σ^2 сохраняет $\zeta_0 + \zeta_2 + \ldots + \zeta_{14}$, а также $\zeta_1 + \zeta_3 + \ldots + \zeta_{15}$ ($p = 17$). Натянутое на них поле квадратично над $\mathbb{Q}$. Легко проверить, что это есть поле $\mathbb{Q}(\sqrt{17})$.