Лекция 19

Пусть R – коммутативное ассоциативное кольцо с единицей, $a \in R$ и $f(x) \in R[x]$. Положим $y = x - a$, тогда $x = y + a$. Если подставить это в $f(x)$ и раскрыть скобки, то получится многочлен $\widetilde{f}(y) = f(y+a)$. Подставим обратно $y = x - a$. Получим *разложение* $f(x)$ *по степеням* $x - a$, то есть выражение вида

$$f(x) = b_n(x-a)^n + b_{n-1}(x-a)^{n-1} + \ldots + b_0.$$

При этом $f(a) = b_0$.

Пример 1. *Пусть $F = \mathbb{R}$, $a = 2$, $f(x) = 3x^2 + 2x + 4$. Тогда*

$$\widetilde{f}(y) = f(y+2) = 3(y+2)^2 + 2(y+2) + 4 = 3y^2 + 14y + 20.$$

То есть $f(x) = 3(x-2)^2 + 14(x-2) + 20$.

Лемма 1 (Лемма Даламбера)**.** *Пусть $z_0 \in \mathbb{C}$, $f(z) \in \mathbb{C}$, $\deg f(z) > 0$ и пусть $f(z_0) \neq 0$. Тогда для любого $\varepsilon > 0 \in \mathbb{R}$ существует $z \in U_\varepsilon(z_0)$ такое, что $|f(z)| < |f(z_0)|$.*

Доказательство. Разложим $f(z)$ по степеням $z - z_0$:

$$f(z) = c_0 + c_k(z-z_0)^k + \ldots + c_n(z-z_0)^n.$$

При этом $c_0 = f(z_0) \neq 0$. Считаем, что $c_k \neq 0$. Подберем аргумент $z - z_0$ таким образом, чтобы

$$\arg\left(c_k(z-z_0)^k\right) = \pi + \arg(c_0).$$

(Ясно, что это возможно сделать верно подобрав $\arg(z - z_0)$ Далее будем подбирать модуль числа $z - z_0$ (в пределах ε-окрестности). Для этого фиксируем некоторое $\widetilde{z}$ с подходящим аргументом $\widetilde{z} - z_0$ и положим $z - z_0 = t(\widetilde{z} - z_0), t \in \mathbb{R}_{>0}$. Получаем

$$\begin{aligned} f(z) = c_0 + c_k(z-z_0)^k + \ldots + c_n(z-z_0)^n = \\ &= c_0 + c_k t^k(\widetilde{z}-z_0)^k + \ldots + c_n t^n(\widetilde{z}-z_0)^n = \\ &= c_0 + c_k t^k(\widetilde{z}-z_0)^k + t^{k+1}(c_{k+1}(\widetilde{z}-z_0)^{k+1} + \ldots + t^{n-k-1}c_n(\widetilde{z}-z_0)^n)). \end{aligned}$$

Оценим модуль $f(z)$:

$$\begin{aligned} |f(z)| \le |c_0 + c_k t^k(\widetilde{z}-z_0)^k| + \\ &+ t^{k+1}|c_{k+1}(\widetilde{z}-z_0)^{k+1} + \ldots + c_n t^{n-k-1}(\widetilde{z}-z_0)^n| \le \\ &\le |c_0 + c_k t^k(\widetilde{z}-z_0)^k| + t^{k+1}(|c_{k+1}(\widetilde{z}-z_0)^{k+1}| + \ldots + |c_n t^{n-k-1}(\widetilde{z}-z_0)^n|) \end{aligned}$$

Пусть $|\widetilde{z} - z_0| = A < 1$ и пусть $\max|c_i| = B$. Тогда $|c_0 + c_k t^k(\widetilde{z}-z_0)^k| = |c_0| - |c_k|t^k A^k$ (считаем $|c_0| > |c_k|t^k A^k$) и $|c_p t^{p-k-1}(\widetilde{z}-z_0)^p| \le B$. В итоге

$$|f(z)| \le |c_0| - |c_k|t^k A^k + t^{k+1}nB = |f(z_0)| - t^k(|c_k|A^k - tnB).$$

Можно подобрать $0 < t < \varepsilon$ так, чтобы $|c_k|A^k - tnB > 0$. □

Теорема 1 (Теорема Безу)**.** *Пусть R – коммутативное ассоциативное кольцо с единицей, $a \in R$ и $f(x) \in R[x]$. Тогда $f(a) = 0$ тогда и только тогда, когда существует представление $f(x) = (x-a)q(x)$.*

Доказательство. Пусть $f(x) = (x-a)q(x)$, тогда $f(a) = 0q(a) = 0$.

Обратно, $f(x) = b_n(x-a)^n + b_{n-1}(x-a)^{n-1} + \ldots + b_0$, где $b_0 = f(a)$. Значит, если $f(a) = 0$, то

$$f(x) = b_n(x-a)^n + b_{n-1}(x-a)^{n-1} + \ldots + b_1(x-a) = = (x-a)(b_n(x-a)^{n-1} + b_{n-1}(x-a)^{n-2} + \ldots + b_1).$$

□

Замечание 1. Если R – область целостности, то $\deg q(x) = \deg f(x) - 1$.

Определение 1. Будем говорить, что многочлен $f(x)$ имеет корень a кратности k, если $f(x)$ может быть представлен в виде $f(x) = (x-a)^k s(x)$ и не может быть представлен в виде $(x-a)^{k+1}r(x)$.

Следствие 1. *Любой многочлен $f \in \mathbb{C}[z]$ степени n раскладывается на линейные множители с коэффициентами из $\mathbb{C}$.*

Доказательство. Индукция по $n = \deg f$. База $n = 1$. Линейный многочлен уже разложен на линейные множители.

Шаг. Пусть z_0 – корень $f(z)$. Тогда $f(z) = (z - z_0)q(z)$. По предположению индукции $q(z)$ раскладывается на линейные множители. Тогда и $f(z)$ тоже. □

Следствие 2. *Любой многочлен с комплексными коэффициентами имеет не менее n корней с учётом кратностей.*

Замечание 2. На самом деле сумма кратностей корней любого комплексного многочлена равна n. Однако это не совсем очевидно из уже доказанного. Тут хочется использовать то, что если

$$f(x) = a(x - x_1)^{k_1} \dots (x - x_m)^{k_m},$$

то кратность корня x_i равна именно k_i. (Чисто теоретически она может быть больше. Вдруг есть другое разложение, где степень вхождения $(x - x_i)$ больше?) Но мы скоро докажем, что разложение многочлена над полем не неприводимые множители единственно, и из этого будет следовать нужное равенство.

Предложение 1. *Пусть z – комплексный корень многочлена $f(x) \in \mathbb{R}[x]$. Тогда $\overline{z}$ – также корень f.*

Доказательство.

$$f(\overline{z}) = a_n\overline{z}^n + \dots + a_0 = \overline{a_n}\,\overline{z}^n + \dots + \overline{a_0} = \overline{f(z)} = \overline{0} = 0.$$

□

Следствие 3. *Любой многочлен с вещественными коэффициентами раскладывается в произведение линейных и квадратичных с отрицательным дискриминантом множителей.*

Доказательство. Индукция по степени многочлена. База $\deg f = 0$ и $\deg f = 1$ очевидна. Пусть $f(x) \in \mathbb{R}[x]$. Если $f(x)$ имеет вещественный корень c, то $f(x) = (x - c)g(x)$, при этом $\deg g < \deg f$ и к g можно применить предположение индукции.

Пусть теперь у $f(x)$ есть комплексный корень λ. Тогда $\overline{\lambda}$ – также корень $f(x)$. Значит, $f(x) = (x - \lambda)(x - \overline{\lambda})h(x)$. При этом $(x - \lambda)(x - \overline{\lambda}) = x^2 - 2\mathrm{Re}\lambda + |\lambda|^2$. При этом дискриминант равен $D = 4(\mathrm{Re}\lambda)^2 - 4|\lambda|^2 < 0$. К h можно применить предположение индукции. □

Многочлены над полем можно делить с остатком.

Предложение 2. *Пусть f и g – многочлены из $F[x]$, где F – некоторое поле. Тогда существуют единственные многочлены $q(x)$ и $r(x)$ такие, что либо $r = 0$, либо $\deg r < \deg g$ и выполнено*

$$f(x) = q(x)g(x) + r(x).$$

Доказательство. Докажем существование индукцией по $\deg f$. База $\deg f < \deg g$. Тогда можно положить $q = 0, r = f$.

Шаг индукции. Пусть $f(x) = a_nx^n + \dots + a_0$ и $g(x) = b_mx^m + \dots + b_0$. Если $n \geq m$, то рассмотрим $h(x) = f(x) - \frac{a_n}{b_m}x^{n-m}g(x)$. Так как $\deg h < \deg f$, по предположению индукции $h(x) = s(x)g(x) + r(x)$, где либо $r = 0$, либо $\deg r < \deg g$. Тогда

$$f(x) = h(x) + \frac{a_n}{b_m}x^{n-m}g(x) = \left(s(x) + \frac{a_n}{b_m}x^{n-m}\right)g(x) + r(x).$$

Докажем единственность. Допустим, что $f = q_1g + r_1 = q_2g + r_2$. Тогда

$$(q_1 - q_2)g = r_2 - r_1.$$

Если $r_1 \neq r_2$, то $\deg(r_2 - r_1) < \deg g \leq \deg(q_1 - q_2)g$. Противоречие. □

Пусть $f = a_nx^n + \dots + a_0 \in R[x]$ – многочлен с коэффициентами из области целостности R. В этот многочлен можно подставлять элементы из R и тогда значение многочлена будет лежать также в R. Таким образом любой многочлен f задаёт функцию $R \to R$. Обозначим эту функцию φ_f. Легко видеть, что отображение $f \to \varphi_f$ – гомоморфизм, то есть при сложении многочленов функции также складываются, а при умножении многочленов – умножаются. Однако данный гомоморфизм из пространства многочленов в пространство функций может быть не инъективным. В самом деле, если R – конечная область целостности, то многочлен

$$f(x) = \prod_{r \in R}(x - r)$$

задаёт тождественно нулевую функцию $R \to R$, хотя сам многочлен не нулевой.

Пример 2. *Пусть p – простое число. По малой теореме Ферма многочлены x^p и x задают одну и ту же функцию на поле $\mathbb{Z}_p$.*

Таким образом стоит различать формальное равенство многочленов (все коэффициенты одинаковые) и функциональное равенство многочленов (задают одну и ту же функцию). Конечно же из формального равенства всегда следует функциональное. Обратное, как мы видели, не верно. Однако для бесконечных областей целостности это верно.

Теорема 2. *Пусть R – бесконечная область целостности. Тогда из функционального равенства многочленов из $R[x]$ следует формальное равенство.*

Доказательство. Пусть два не равных формально многочлена f и g из $R[x]$ функционально равны. Рассмотрим их расность. Это многочлен $h(x) = f(x) - g(x)$ с ненулевыми коэффициентами, задающий тождественно нулевую функцию. Пусть степень f равна m. Возьмём различные элементы $c_1, \dots, c_m \in R$. Так как $h(c_1) = 0$, мы получаем $h(x) = (x - c_1)h_1(x)$. Подставим в это выражение c_2, получим $0 = h(c_2) = (c_2 - c_1)h_1(c_2)$. Так как $c_1 \neq c_2$ и R без делителей нуля, получаем $h_1(c_2) = 0$. Тогда $h(x) = (x - c_1)(x - c_2)h_2(x)$. Продолжая таким образом, получим $h(x) = a_n(x - c_1) \dots (x - c_n)$. Но подставив c_{n+1} в это выражение, мы не получим ноль. Противоречие. $\square$