3. Корни многочленов. Теорема Безу. Формальная производная. Кратные корни.

Определение 1. Пусть $P \in F[x]$. Скаляр $a \in F$ называется ***корнем многочлена*** P, если $P(a) = 0$.

Теорема 1. (Безу). $a \in F$ — корень $P \in F[x] \Leftrightarrow (x-a)|P$.

▲ Разделим P с остатком на $(x-a) : P = Q(x-a) + R, degR. \leqslant 0$ ($degR$ - степень многочлена R) Заметим, что $P(a) = R$, тогда $P(a) = 0 \Leftrightarrow R = 0 \Leftrightarrow (x-a)|P$. ■

Определение 2. Пусть $a \in F$ - корень $P \in F[x]$. ***Кратностью корня*** a называется наибольшее $\gamma \in \mathbb{N}$ такое, что $(x-a)^\gamma|P$. Если $\gamma > 1$, то корень а называется *кратным*, иначе — *простым*.

Теорема 2. Пусть $P \in F[x]$ — ненулевой многочлен, $a_1, \ldots, a_k$ — его корни, $\gamma_1, \ldots, \gamma_k$ — их кратности. Тогда $\gamma_1 + \ldots + \gamma_k \leqslant degP$.

▲ $\forall i \in 1, \ldots, k : (x-a_i)^{\gamma_i}|P$. Кроме того, $\forall i, j \in \{1, \ldots, k\}, i \neq j :$ НОД$(x-a_i, x-a_j) =$ НОД$(x-a_i, a_i-a_j) = 1$, значит, все многочлены вида $(x-a_i)^{\gamma_i}$ попарно неассоциированны, тогда все они входят в разложение P на неприводимые сомножители, поэтому $\gamma_1+\ldots+\gamma_k \leqslant degP$. ■

Замечание. В нецелостном кольце данная теорема неверна, поскольку неверна единственность разложения на неприводимые сомножители. Например, в $\mathbb{Z}_4$ у многочлена $P = x^2 = (x-2)^2$ есть корень 0 кратности 2 и корень 2 кратности 2, при этом $degP = 2$.

Замечание. Над полем $\mathbb{C}$ у каждого многочлена число корней с учетом кратности равно его степени, поскольку, согласно основной теореме алгебры, $\forall P \in \mathbb{C}[x], degP > 1 : P$ есть корень.

Определение 3. Пусть $P \in F[x], P(x) = p_0 + p_1x + \ldots + p_nx^n$. ***Формальной производной*** многочлена $P(x)$ называется многочлен $P'(x) = p_1 + 2p_2x + \ldots + np_nx^{n-1}$, где скаляры $2, \ldots, n$ — это суммы соответствующего числа единиц.

Утверждение 1. Пусть $P, Q \in F[x]$. Тогда:

1. $\forall \alpha, \beta \in F : (\alpha P + \beta Q)' = \alpha P' + \beta Q'$ (формальная производная — это линейное преобразование пространства многочленов)

2. $(PQ)' = P'Q + PQ'$

▲

1. Пусть$n = max(degP, degQ)$, тогда$P = \sum_{i=0}^n p_ix^i, Q = \sum_{i=0}^n q_ix^i, \alpha P + \beta Q = \sum_{i=0}^n (\alpha p_i + \beta q_i)x^i$. Проверим равенство непосредственной проверкой:
   $(\alpha P + \beta Q)' = \sum_{i=1}^n (\alpha p_i + \beta q_i)x^{i-1} = \alpha \sum_{i=1}^n ip_ix^{i-1} + \beta \sum_{i=1}^n iq_ix^{i-1} = \alpha P' + \beta Q'$

2. Левая и правая части линейны по P и по Q, поэтому равенство достаточно проверить на некотором базисе пространства многочленов, т. е. в случае, когда $P(x) = x^i, Q(x) = x^j$:
   $(PQ)' = (i+j)x^{i+j-1} = ix^{i-1}x^j + x^ijx^{j-1} = P'Q + PQ'$ ■

Замечание. Формальная производная не обладает аналитическими свойствами. Над полем $\mathbb{Z}_p$, например, $(x^p)'px^{p-1} \equiv 0$.

Следствие.

1. $(P_1P_2 \ldots P_n)' = P_1'P_2 \ldots P_n + P_1P_2' \ldots P_n + \ + P_1P_2 \ldots P_n'$

2. $(P^n)' = nP^{n-1}P'$

3. $(P(Q))' = P'(Q)Q'$

▲

1. Данное утверждение является прямым следствием предыдущего с применением индукции по n.

2. Достаточно применить первое равенство к $P^n = P \cdot \ldots \cdot P$.

3. Считая, что $P(x) = p_0 + p_1 x + \ldots + p_n x^n$, воспользуемся вторым равенством: $(P(Q))' = (\sum_{i=1}^{m}(p_i Q^i))' = \sum_{i=1}^{m} i p_i Q^{i-1} Q' = P'(Q)Q'$ ■

Теорема 3. Пусть $P \in F[x], c \in F$. Тогда c — кратный корень $P \Leftrightarrow P(c) = P'(c) = 0 \Leftrightarrow (x-c)|\text{НОД}(P, P')$.

▲ Докажем сначала первую равносильность. Рассмотрим c — корень P, $P = (x-c)Q$, тогда $P' = Q + (x-c)Q'$ поэтому c — кратный корень $P \Leftrightarrow Q(c) = 0 \Leftrightarrow P'(c) = 0$.

Теперь докажем вторую равносильность:

$$\begin{cases} P(c) = 0 \\ P'(c) = 0 \end{cases} \Leftrightarrow \begin{cases} (x-c)|P \\ (x-c)|P' \end{cases} \Leftrightarrow (x-c) \mid \text{НОД}(P, P') \quad ■$$

Теорема 4. Пусть $c \in F$ — корень $P \in F[x]$ кратности k. Тогда c — корень P' кратности хотя бы $k-1$. Более того, если $charF > k$ или $charF = 0$ ($charF$ - наименьшее целое $n > 0$ такое, что для каждого элемента $r \in F$ выполняется равенство: $r + \ldots + r (n \text{ раз}) = 0$, а если такого числа не существует, то предполагается $charR = 0$), то c — корень P' кратности ровно $k-1$.

▲ P имеет вид $(x-c)^k Q'$, причем $(x-c) \nmid Q$. Тогда: $P' = k(x-c)^{k-1}Q + (x-c)^k Q' = (x-c)^{k-1}(kQ + (x-c)Q')$ Из данного равенства уже следует, что c — корень P' кратности хотя бы $k-1$. Теперь поделим P' на $(x-c)^{k-1}$ и получим $kQ + (x-c)Q'$. Если $charF > k$ или $charF = 0$, то $kQ(c) \neq 0$, поэтому кратность корня c у многочлена P равна $k-1$. ■

Следствие.

1. Если $c \in F$ — корень $P \in F[x]$ кратности k, то $P(c) = P'(c) = \ldots = P^{(k-1)}(c) = 0$.

2. Если $P(c) = \ldots = P^{(k-1)}(c) = 0$ и $charF > k$ или $charF = 0$. Тогда c — корень P кратности хотя бы k.

▲

1. Последовательно применим предыдущую теорему к P, P' и т. д.: $(x-c)^k|P \Rightarrow (x-c)^{k-1}|P' \Rightarrow \ldots \Rightarrow (x-c)|\ P^{(k-1)}$.

2. Предположим противное: пусть c — корень кратности $l < k$ у P. Тогда c — корень кратности $l-1$ у $P', \ldots$, простой корень у $P^{(l-1)}$, но тогда $P^l(c) \neq 0$ — противоречие. ■