Неприводимые многочлены и их свойства. Теорема о разложении в произведение неприводимых многочленов. Каноническое разложение.

Неприводимый многочлен $f(x) \in F[x]$ называется неприводимым над полем F, если его нельзя разложить в произведение многочленов меньшей степени, то есть если $\forall f(x) = g(x)h(x)$ либо $\deg g(x) = \deg f(x)$, либо $h(x) = \deg f(x)$
Разложимый многочлен Многочлен $f(x) \in F[x]$ приводим (разложим) над полем F, если существует $f(x) = g(x)h(x)$, где $g(x), h(x) \in F[x]$

Теорема о разложении многочлена в произведение неприводимых многочленов

Каждый многочлен однозначно раскладывается в произведение неприводимых многочленов, с точностью до перестановки сомножителей и ассоциированности.
Доказательство существования
Докажем индукцией по степени многочлена.

1. Если $f(x)$ - неприводим, то $f(x) = f(x)$
2. Пусть доказано для многочленов степени меньше m. При этом, если $f(x)$ разложим, то $f(x) = g(x)h(x)$. При этом $\deg g(x), \ \ \deg h(x) < \deg f(x)$, т.к. по предположению индукции $g(x)$ и $h(x)$ раскладываются в произведение неприводимых многочленов.

Доказательство единственности
Предположим, что есть два разложения для $f(x)$:

$$f(x) = g_1(x) \dots g_k(x) = h_1(x) \dots h_m(x)$$

Так как $g_1(x)$ неприводим и $g_1(x) \mid h_1(x) \dots h_m(x)$, то по доказанному выше предложению существует j такое, что $g_1(x) \mid h_j(x)$. Перенумеруем $h(x)$ и будем считать $j = 1$. Тогда $g_1(x) \mid h_1(x)$. Так как $h_1(x) = q(x)g_1(x)$ и $h_1(x)$ неприводим, то $\deg h_1(x) = \deg g_1(x)$, то есть $h_1(x)$ и $g_1(x)$ ассоциированы.

$$g_1(x)g_2(x) \dots g_k(x) = cg_1(x)h_2(x) \dots h_m(x)$$

Получаем

$$g_2(x) \dots g_k(x) = ch_2(x) \dots h_m(x)$$

И продолжаем аналогичный процесс. Мы найдём для $g_2(x)$ ассоциированный многочлен $h_2(x)$, далее для $g_3(x)$, и т.д.

Предложение о неприводимых многочленах
Пусть g неприводим над полем F и $g \mid (h_1(x)h_2(x) \dots h_m(x))$. Тогда существует число i такое, что $g \mid h_i(x)$

Доказательство
Б.И. - для $m = 1$ - очевидно

Ш.И. Предположим, что утверждение доказано для случая, когда менее m сомножителей.
Рассмотрим случай m сомножителей. Пусть $d(x) = \text{НОД}(g(x), h_m(x))$. Тогда $\exists q(x) : g(x) = q(x)d(x)$. По условию теоремы g - неприводим, поэтому возможны два случая:

1. $\deg d(x) = \deg g$, тогда $g(x)$ и $g(x)$ - ассоциированы.
2. Если $d(x) = 1$, тогда $g(x)$ и $h_m(x)$ - взаимно просты, и, по доказанной лемме, $g(x) \mid h_1(x) \cdot \dots \cdot h_{m-1}(x)$. Тогда по предположению индукции получаем, что найдётся i такое, что $g(x) \mid h_i(x)$

Каноническое разложение Любой многочлен можно представить в виде $f(x) = a(x - x_1)(x - x_n)$, где x_n - корни, а $(x - x_1) \dots (x - x_n)$ неприводимые члены