Einstein's Criterion of Irreducibility

Th^m: Let F be the field of quotients of a unique factorisation domain R. If

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$$

and p is a prime element of R such that

$$p \mid a_0,\ p \mid a_1,\ p \mid a_2 \cdots\ p \mid a_{n-1}$$

whereas p is not a divisor of a_n and p^2 is not a divisor of a_0, then $f(x)$ is irreducible in $F[x]$.

Proof Without loss of generality, we may take $f(x)$ to be a primitive, as taking out the GCD of its coefficient does not disturb the hypothesis, since p is not a divisor of a_n.

Now let $f(x)$ is reducible in $F[x]$. Then $f(x)$ can be factored as the product of two polynomials of positive degree in $F[x]$. Therefor by Gauss Lemma $f(x)$ can ~~f~~ be factorised as product of two polynomials of positive degree in $R[x]$

Thus if we assume that $f(x)$ is reducible in $F[x]$, then

$$f(x) = a_0 + a_1x + \cdots + a_nx^n = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s) \quad \text{—— (1)}$$

where b_i's & c_j's are elements of R and $r>0$, $s>0$

From (1) $\quad a_0 = b_0c_0$

Since p is a prime element of R, therefor

$$p \mid a_0 \Rightarrow p \mid b_0 \text{ or } p \mid c_0$$

Also p^2 is not a divisor of a_0, therefore p cannot divide both b_0 & c_0.

Let us suppose that $p \mid b_0$ & p is not divisor of c_0. Also p cannot divide all the coefficients $b_0, b_1, \cdots b_r$ because if p divides all the coefficients $b_0, b_1, \cdots b_r$ then p will ~~still~~ divide all the coefficients of $f(x)$ which is not true as p does not divide a_n. Let b_K where $K \leq r$ be the first b_i which is not divisible by p. Then each of $b_0, b_1, \cdots b_{K-1}$ is divisible by p and b_K is not divisible by p.

Also $k < n$ since $r < n$

Now from (1) we have

$$a_K = b_K c_0 + b_{K-1} c_1 + \cdots + b_0 c_K$$

$$\Rightarrow b_K c_0 = a_K - b_{K-1} c_1 - b_{K-2} c_2 - \cdots - b_0 c_K) \quad \text{——} (2)$$

Now $K < n$ therefore $p \mid a_K$. Also $p \mid b_{K-1}, b_{K-2}, \cdots b_0$

Therefore from (2)

$$p \mid b_K c_0$$

$\Rightarrow p \mid b_K$ or $p \mid c_0$, since p is prime element of R.

Which is absurd as our assumption is p is neither a divisor of b_K nor a divisor of c_0

Hence $f(x)$ must be irreducible in $F[x]$.

Proved

Note: If in the above theorem, we take ring of integers I in place of UFD 'R', then field of quotients is field of rational numbers.

So above theorem can be stated as:

Let $f(x) = a_0 + a_1 x + \cdots a_n x^n$ be a polynomial with integer coefficients. If p is prime number such that

$$p \mid a_0,\ p \mid a_1,\ \ldots,\ p \mid a_{n-1}$$

Where as p does not divide a_n & p^2 does not divide a_0 the $f(x)$ is irreducible over the field of rational numbers.

Ex ① If p is a prime number, prove that the polynomial $x^n - p$ is irreducible over the field of rational numbers.

Solⁿ Here $f(x) = -p + 0.x + 0.x^2 + \cdots + 0x^{n-1} + 1.x^n$.

Here $f(x)$ is polynomial with integral coefficients and p is a prime.

Since p divides all the coefficient of $f(x)$ except the coefficient of last term x^n. and also p^2 does not divide the first coefficient $(-p)$. Hence, by Einstein's Criterion of irreducibility, $f(x)$ is irreducible over field of rational numbers.

Ex ② ~~Prove~~ Show that the polynomial $x^3 - 3$ is irreducible over field of rational numbers.

Solⁿ Same as above