November 27th, 2015

Remark on Exercise class of November 27th

Dr. V. Di Proietto

Theorem 1. *Every irreducible and primitive polynomial in $\mathbb{Z}[X]$ is irreducible in $\mathbb{Q}[X]$.*

Proof. Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ be an irreducible and primitive polynomial in $\mathbb{Z}[X]$, in particular $a_i \in \mathbb{Z}$, and let us suppose that $f(X) = g(X)h(X)$ in $\mathbb{Q}[X]$ with $g(X)$ and $h(X)$ not units in $\mathbb{Q}[X]$. Then there exists $\alpha \in \mathbb{Z}$ such that $\alpha g(X)$ is a polynomial in $\mathbb{Z}[X]$. We consider the greatest common divisor d of the coefficients of $\alpha g(X)$, then $\gamma(X) = \frac{\alpha}{d} g(X)$ is an element of $\mathbb{Z}[X]$ which is primitive. We do the same with $h(X)$: there exists an integer β such that $\beta h(X)$ is in $\mathbb{Z}[X]$. Then we take d' the greatest common divisor of the coefficients of $\beta h(X)$, hence $\eta(X) = \frac{\beta}{d'} h(X)$ is a primitive polynomial in $\mathbb{Z}[X]$. Now

$$\frac{\alpha}{d}\frac{\beta}{d'} f(X) = \gamma(X)\eta(X) \tag{1}$$

is a primitive polynomial of $\mathbb{Z}[X]$ because of ex 1 (v). We want to prove that

$$\frac{\alpha}{d}\frac{\beta}{d'} = \frac{A}{B}$$

is in $\mathbb{Z}$. Suppose the rational number $\frac{A}{B}$ is not in $\mathbb{Z}$, then there exists a prime number p such that $p \mid B$ but $p \nmid A$. But

$$\frac{A}{B} f(X) = \frac{A}{B} a_0 + \frac{A}{B} a_1 X + \cdots + \frac{A}{B} a_n X^n$$

is in $\mathbb{Z}[X]$. Hence

$$\frac{A}{B} a_i$$

is in $\mathbb{Z}$ for every $i = 0, \ldots, n$, hence $p \mid A a_i$ for every $i = 0, \ldots, n$, and $p \nmid A$ so $p \mid a_i$ for every $i = 0, \ldots, n$, but this is not possible because $f(X)$ was supposed to be primitive. Hence $\frac{A}{B}$ is in $\mathbb{Z}$. Since $\frac{A}{B} f(X)$ is primitive, then $\frac{A}{B} = \pm 1$. Hence equation (1) becomes

$$f(X) = \pm \gamma(X)\eta(X)$$

But since by hypothesis $f(X)$ is irreducible in $\mathbb{Z}[X]$, then this implies that $\gamma(X)$ or $\eta(X)$ is a unit of $\mathbb{Z}[X]$. Therefore since $\eta(X) = \frac{\beta}{d'} h(X)$ and $\gamma(X) = \frac{\alpha}{d} g(X)$ this implies that $h(X)$ and $g(X)$ are units in $\mathbb{Q}[X]$ which is a contradiction. $\square$