Math 122 Wednesday, December 7

$f(x) \in R = \mathbb{Z}[x]$ is a unique factorization domain (but not a PID so not Euclidean)

$\mathbb{Z}[x] \subset \mathbb{Q}[x]$ which is Euclidean so $f(x)$ has a unique factorization into irreducible monic polynomials: $f(x) = u\, p_1(x) \cdots p_r(x)$, u = unit in $\mathbb{Q}^*$, $p_i(x)$ irred monic poly in $\mathbb{Q}[x]$. Each $p_i(x) = c_i q_i(x)$ with $c_i \in \mathbb{Q}^*$, $q_i(x) \in \mathbb{Z}[x]$ primitive so $f(x) = (u \prod c_i)\, q_1(x) \cdots q_r(x) = c\, q_1(x) \cdots q_r(x)$. Only worry is that $c \in \mathbb{Q}^* \setminus \mathbb{Z}$ but $c \in \mathbb{Z}$ as $f(x) \in \mathbb{Z}[x]$ and $f(x) = c \cdot$ (primitive poly) (primitive by Gauss' lemma). Factor $c = \pm p_1 \cdots p_k \Rightarrow f(x) = \pm p_1 \cdots p_k\, q_1(x) \cdots q_r(x)$ Done.

Note: Gauss' Lemma is crucial to the above argument. Because of its importance, we review the proof.

Gauss' Lemma If $f(x)$ and $g(x)$ are primitive in $\mathbb{Z}[x]$ so is $f(x)g(x)$.

Pf: $f(x)g(x)$ is primitive $\iff$ no prime p divides all of its coefficients $\iff$ $\overline{f}(x)\overline{g}(x) = \overline{f(x)\,g(x)}$ is nonzero for all p where $f(x) \longmapsto \overline{f}(x) = f(x) \bmod p$ via the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$. We knows $\overline{f}, \overline{g} \neq 0$ in $\mathbb{Z}/p\mathbb{Z}[x]$ as these are primitive. So $\overline{f}(x) = a_n x^n + \cdots$, $\overline{g}(x) = b_m x^m + \cdots$ $a_n, b_m \not\equiv 0 \pmod p$. So $\overline{f}(x)\overline{g}(x) = a_n b_m x^{n+m} + \cdots \neq 0$ as $a_n b_m \neq 0$ as $\mathbb{Z}/p\mathbb{Z}$ is a domain.

Corollary If $f(x)$ is primitive, $g(x)$ arbitrary in $\mathbb{Z}[x]$, then $g(x) = f(x)\,m(x)$ a factorization in $\mathbb{Q}[x] \Rightarrow m(x)$ is in $\mathbb{Z}[x]$.

Pf: $g(x) = f(x) \cdot c \cdot m_0(x)$ with $m_0(x) \in \mathbb{Z}[x]$ primitive $\Rightarrow g(x) = c \cdot f(x)\, m_0(x)$. $f(x)\, m_0(x) \in \mathbb{Z}[x]$ is primitive by Gauss' lemma $\Rightarrow c \in \mathbb{Z} \Rightarrow m(x) \in \mathbb{Z}[x]$.

Corollary Assume $f(x)$ is non-constant in $\mathbb{Z}[x]$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Pf: ($\Leftarrow$) is obvious. ($\Rightarrow$) Assume $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$. Say $f(x) = g_1(x)\, g_2(x)$ in $\mathbb{Q}[x] \Rightarrow f(x) = c_1 g_1^\circ(x)\, c_2 g_2^\circ(x) = g_1^\circ(x) \cdot (c_1 c_2 g_2^\circ(x))$. First part is primitive in $\mathbb{Z}[x]$ so by previous corollary the last part is in $\mathbb{Z}[x]$.

Surprising fact is that we can use this to prove the irreducibility of polynomials in $\mathbb{Q}[x]$ using reduction (mod p). Consider $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$, $f(x) \in \mathbb{Z}[x]$ a monic polynomial. Then if $\overline{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ is irreducible modulo p, $f(x)$ must be irreducible in $\mathbb{Z}[x]$ for any factorization of f gives a factorization of $\overline{f}$.

ex: $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ (equivalently $\sqrt{2} \notin \mathbb{Q}$).

x^2-2 irred in $\mathbb{Q} \iff x^2 - 2$ irred in $\mathbb{Z}$. Consider $x^2 - 2 \pmod 3$. This factors iff there is a root in $\mathbb{Z}/3\mathbb{Z}$. But $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 1$ so $x^2 - 2$ is irreducible mod $3 \Rightarrow x^2 - 2$ is irreducible in $\mathbb{Z}$ and thus $\mathbb{Q}$.

These are called (mod p) methods on polynomials over $\mathbb{Z}[x]$. There are also a set of p-adic methods for proving irreducibility, the most famous of which is Eisenstein's criterion.

Eisenstein's Criterion Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ such that p divides all of the a_i and p^2 does not divide a_0. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.
Pf: Suppose $f(x) = g(x)h(x)$. Then mod p, $\bar{f}(x) = x^n = \bar{g}(x)\bar{h}(x) \Rightarrow \bar{g}(x) = x^a$, $\bar{h}(x) = x^b$. As $f(x)$ is monic so are $g(x)$ and $h(x)$ so $g(x) = x^a + c_{a-1}x^{a-1} + \cdots + c_0$ and $h(x) = x^b + d_{b-1}x^{b-1} + \cdots + d_0$ where $\bar{g}(x) = x^a$, $\bar{h}(x) = x^b \Rightarrow$ p divides all of the c_i and all of the d_i. But $a_0 = c_0 d_0$ is then divisible by $p^2 \Rightarrow\Leftarrow$. Hence $f(x)$ is irreducible.

Eisenstein developed this criterion to show that cyclotomic polynomials are irreducible. $\alpha = e^{2\pi i/p}$ is algebraic and satisfies the polynomial $(x^p - 1) = (x-1)(x^{p-1} + \cdots + x + 1)$. $\alpha - 1 \neq 0$ so α is a root of $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Thm (Gauss Eisenstein) The polynomial $f(x)$ is irreducible.
Pf: We note that $f(x)$ is irreducible iff $g(x) = f(x+1)$ is irreducible for a factorization of one gives a factorization of the other. By definition $g(x) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1}$. This is an Eisenstein polynomial because if p is prime $p \nmid \binom{p}{k}$ for all $k \in \{1, \ldots, p-1\}$. So $g(x)$ is irreducible $\Rightarrow$ so is $f(x)$.

What is $\bar{f}(x) \pmod{l}$ $l \neq p$ a prime? The degree of the factors of $\bar{f}(x)$ is the order of $l \in (\mathbb{Z}/p\mathbb{Z})^\times$. So if $l = 1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ then $q = l$ and $f(x)$ splits into a product of linears (mod l). This makes sense because $l \equiv 1 \bmod p$ iff $p \mid l - 1$ which means there are p-th roots of unit in $(\mathbb{Z}/l\mathbb{Z})^\times$.