Content:

Example $f(x) = x^2 - x - 2 = \left(\frac{5x}{2} + \frac{5}{2}\right)\left(\frac{2x}{5} - \frac{4}{5}\right) = \frac{5}{2}(x+1)\bullet\frac{2}{5}(x-2) = (x+1)(x-2)$

Theorem (Gauss) If R is a UFD, Q its field of fractions, $f(x) \in R[x]$, $f(x) = G(x)H(x)$ where $G(x), H(x) \in Q[x]$, then $\exists\ g(x), h(x) \in R[x]$ such that deg $G(x)$ = deg $g(x)$ and deg $H(x)$ = deg $h(x)$ and $f(x) = g(x)h(x)$.

Example $f(x) = \frac{1}{3}x^4 - 2x^2 + \frac{1}{8} = \frac{1}{24}(8x^4 - 48x + 3)$

Theorem (mod p test) If $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, p is a prime number, $\bar{f}(x) = [a_0] + [a_1]x + \cdots + [a_n]x^n \in \mathbb{Z}_p[x]$, deg $f(x)$ = deg $\bar{f}(x)$ and $\bar{f}(x)$ is irreducible, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example $f(x) = x^3 + x + 1$ has no roots in $\mathbb{Z}_2$ so $f(x)$ is irreducible.

Theorem Rational Root Test. If $a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $a_n \neq 0$; $r, s \in$ Z, r and s are relatively prime, and r/s is a root of $f(x)$, then $r|a_0$ and $s|a_n$.

Theorem Eisenstein's Criterion. If $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $a_n \neq 0$; and there is p, a prime number, such that $p|a_i\ \forall\ i < n$, $p^2 \nmid a_0$ and $p \nmid a_n$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proposition If $f(x) \in \mathbb{Z}[x]$, and $\exists\ c \in \mathbb{Z}$ such that $f(x + c)$ is irred then $f(x)$ is irreducible.

Example If p is prime and $f(x) = 1 + x + \cdots + x^{p-1}$, then $f(x)$ is irreducible.

Question Does reducibility over $\mathbb{Z} \Rightarrow$ reducibility over $\mathbb{Q}$? No.
$2x + 2$ is reducible over $\mathbb{Z}$, but not over $\mathbb{Q}$. $2x + 2 = 2(x + 1)$.

Question Does reducibility over $\mathbb{Q} \Rightarrow$ reducibility over $\mathbb{Z}$? Yes.

Example $f(x) = x^2 - x - 2 = \left(\frac{5x}{2} + \frac{5}{2}\right)\left(\frac{2x}{5} - \frac{4}{5}\right) = \frac{5}{2}(x+1)\bullet\frac{2}{5}(x-2) = (x+1)(x-2)$
We can always do this.

Theorem (Gauss) Let R be a UFD, Q its field of fractions, $f(x) \in R[x]$. If $f(x) = G(x)H(x)$ where $G(x), H(x) \in Q[x]$, then $\exists\ g(x), h(x) \in R[x]$ such that deg $G(x)$ = deg $g(x)$ and deg $H(x)$ = deg $h(x)$ and $f(x) = g(x)h(x)$.

Proof:
p. 334. Read it.
By Lemma 6.24 (i)(Let R be a UFD, Q = Frac(R), $f(x) \in Q[x]$. Then there is a factorization $f(x) = c(f)f^*(x)$ such that c(f) $\in Q$, $f^*(x)$ is primitive in $R[x]$. This factorization is unique ...), the factorization $f(x) = G(x)H(x)$ in $Q[x]$ give $q, q' \in Q$ with $f(x) = qG^*(x)\ q'H^*(x)$ in $Q[x]$. where $G^*(x), H^*(x) \in R[x]$ are primitive. But $G^*(x)H^*(x)$ is primitive, by Gauss's lemma. Since $f(x) \in R[x]$, Lemma 6.24 (iii) (Let $f(x) \in Q$[x] such that $f(x) = qf^*(x)$ where $q \in Q$ and $f^*(x)$ is primitive in $R[x]$. Then $f(x) \in R[x] \Leftrightarrow q \in R$.) applies to say that the equation $f(x) = qq'[G^*(x)H^*(x)]$ forces $qq' \in R$.
Therefore, $qq'G^*(x) \in R[x]$, and a factorization of $f(x)$ in $R[x]$ is $f(x) = [qq'G^*(x)]H^*(x)$.

Example $f(x) = \frac{1}{3}x^4 - 2x^2 + \frac{1}{8}$ Explore the irreducibility of $f(x)$ in $\mathbb{Q}[x]$.

$f(x) = \frac{1}{3}x^4 - 2x^2 + \frac{1}{8} = \frac{1}{24}(8x^4 - 48x + 3)$.

Suppose we have tools to determine irreducibility of $(8x^4 - 48x + 3)$.

Theorem **(mod p test)**

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, p is a prime number.

Let $\bar{f}(x) = [a_0] + [a_1]x + \cdots + [a_n]x^n \in \mathbb{Z}_p[x]$.

If $\deg f(x) = \deg \bar{f}(x)$ and $\bar{f}(x)$ is irreducible, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof:

Define $\varphi: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ by $\varphi(f(x)) = \bar{f}(x)$.

By contraposition, assume f is reducible over $\mathbb{Q}$ and $\deg f = \deg \bar{f}$.

We will show $\bar{f}(x)$ is reducible in $\mathbb{Z}_p[x]$.

Since $f(x)$ is reducible in $\mathbb{Q}[x]$, then by previous theorem by Gauss, we may assume $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathbb{Z}[x]$ and $\deg g(x) < \deg f(x)$ and $\deg h(x) < \deg f(x)$.

Since φ is a homomorphism, then $\varphi(f(x)) = \varphi(g(x)h(x)) = \varphi(g(x))\varphi(h(x))$.

And since $\deg \varphi(g(x)) \le \deg g(x) < \deg f(x) = \deg \bar{f}(x)$ and $\deg \varphi(h(x)) \le \deg h(x) < \deg f(x) = \bar{f}(x)$, then we have a non-trivial factorization of $\bar{f}(x)$.

So $\bar{f}(x)$ is reducible in $\mathbb{Z}_p[x]$.

Example $f(x) = x^3 + x + 1 \in \mathbb{Z}[x]$.

$\bar{f}(x) = [1]x^3 + [1]x + [1]$ has no roots in $\mathbb{Z}_2$ so $\bar{f}(x)$ is irreducible, hence $f(x)$ is irreducible by mod p test.

Theorem **Rational Root Test (Thm 3.43, p. 141)**

Let $a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $a_n \neq 0$.

If $r, s \in \mathbb{Z}$, r and s are relatively prime, and r/s is a root of $f(x)$, then $r|a_0$ and $s|a_n$.

Proof:

$0 = f(r/s) = a_0 + a_1(r/s) + \cdots + a_n(r/s)^n = a_0s^n + a_1rs^{n-1} + \cdots + a_nr^n$.

So $a_nr^n = -a_0s^n - a_1rs^n - \cdots - a_{n-1}r^{n-1}s$.

So $s|a_nr^n$. Since s, r are relatively prime, it follows that s and r^n are relatively prime and so Euclid's lemma in $\mathbb{Z}$ gives $s|a_n$.

Similarly $a_0s^n = -a_1rs^n - \cdots - a_{n-1}r^{n-1}s - a_nr^n$, and $r|a_0$.

Theorem **Eisenstein's Criterion.**
Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $a_n \neq 0$. If there is a prime number, p, such that $p|a_i \ \forall\ i < n$, $p^2 \nmid a_0$ and $p \nmid a_n$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof:
By contraposition, assume $f(x)$ is reducible over $\mathbb{Q}$, $p|a_i \ \forall\ i < n$, and $p \nmid a_n$. We will show $p^2 \mid a_0$.
Since $f(x)$ is reducible in $\mathbb{Q}[x]$, then by previous theorem by Gauss, we may assume $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathbb{Z}[x]$ and $\deg g(x) < \deg f(x)$ and $\deg h(x) < \deg f(x)$.
Define $\varphi: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ by
$\varphi(f(x)) = \bar{f}(x) = [a_0] + [a_1]x + \cdots + [a_n]x^n \in \mathbb{Z}_p[x]$.
So we have $\bar{f}(x) = \varphi(f(x)) = \varphi(g(x))\varphi(h(x)) = \bar{g}(x)\,\bar{h}(x)$ in $\mathbb{Z}_p[x]$.
Since $p|a_i \ \forall\ i < n$ and $p \nmid a_n$, then we know
$\bar{f}(x) = [a_n]x^n = [a_n]x \bullet x \bullet\bullet\bullet$ where a_n is a unit in $\mathbb{Z}_p$ and $[a_n] \neq 0$,
By Thm 3.42 (Unique Factorization: If k is a field, then every polynomial $f(x) \in k[x]$ of degree $\geq 1$is a product of a nonzero constant and monic irreducibles. Moreover, if $f(x) = ap_1(x)\cdots p_m(x)$ and $f(x) = bq_1(x)\cdots q_n(x)$, where a and b are nonzero constants and the p's and q's are monic irreducibles, then $a = b$, $m = n$, and the q's may be reindexed so that $q_i = p_i$ for all i), we must have that $\bar{g}(x) = [b_m]x^m$ and $\bar{h}(x) = [c_k]x^k$ where $[b_m]$, $[c_k]$ are units in $\mathbb{Z}_p$ and $m + k = n$.
Note that $g(x) = b_0 + b_1x + \cdots + b_mx^m$ and $h(x) = c_0 + c_1x + \cdots + c_kx^k$.
Since $\bar{g}(x) = [b_m]x^m$, it follows that $[b_0] = 0$. So $p|b_0$. Similarly $p|c_0$.
$p|b_0$, $p|c_0$ and p prime $\Rightarrow p^2|b_0c_0$. Thus $p^2|a_0$.

Proposition Let $f(x) \in \mathbb{Z}[x]$. If $\exists\ c \in \mathbb{Z}$ such that $f(x + c)$ is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof:
By contraposition, assume $f(x)$ is reducible over $\mathbb{Q}$.
We will show $f(x + c)$ is reducible.
Since $f(x)$ is reducible over $\mathbb{Q}$ then by previous theorem by Gauss, we can assume $g(x), h(x) \in \mathbb{Z}[x]$ where $\deg g(x) < \deg f(x)$ and $\deg h(x) < \deg f(x)$.
Define $\varphi: \mathbb{Z}[x] \to \mathbb{Z}[x]$ by $\varphi(f(x)) = f(x + c)$.
We have proven previously that φ is a ring homomorphism.
Note that $\deg f(x) = \deg (f(x))$.
So $f(x + c) = \varphi(f(x)) = \varphi(g(x))\varphi(h(x))$ where $\deg \varphi(g(x)) < \deg f(x + c)$ and $\deg \varphi(h(x)) < \deg f(x + c)$. Thus, $f(x + c)$ is reducible.
$\therefore$ By contraposition $f(x + c)$ irreducible $\Rightarrow f(x)$ irreducible.

Example Let p be prime and $f(x) = 1 + x + \cdots + x^{p-1}$, then $f(x)$ is irreducible.

Proof:

$f(x) = \dfrac{x^p - 1}{x - 1}$. So $f(x+1) = \dfrac{(x+1)^p - 1}{x} = \dfrac{x^p + \binom{p}{p-1}x^{p-1} + \cdots + \binom{p}{2}x^2 + \binom{p}{1}x + 1 - 1}{x} =$

$x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}$.

So, by Eisenstein, $f(x + 1)$ is irreducible. $\therefore$ $f(x)$ is irreducible.