Recall: Let $f(x)$ is a monic polynomial with integer coefficients. Then $f(x)$ factors as a product of polynomials of degrees n and m if and only if $f(x)$ factors as a product of polynomials of degrees n and m in $\mathbb{Z}[x]$.

Corollary: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $a_0 \neq 0$. If $f(x)$ has a root in $\mathbb{Q}$, then $f(x)$ has a root $\alpha \in \mathbb{Z}$ and $\alpha \mid a_0$.

Definition: Let F be a field and $f(x) \in F[x]$ with $\deg(f(x)) \geq 1$. Then $f(x)$ is irreducible over F if $f(x)$ cannot be expressed as a product of two polynomials of degree ≥ 1 in $F[x]$

Example: Show that $f(x) = x^4 - 5x^2 + 1$ is irreducible over $\mathbb{Q}$.

Observe that if $f(x)$ is reducible, then $f(x) = g(x)h(x)$. We have two cases:

Case 1: $\deg(h(x)) = 1$ and $\deg(g(x)) = 3$. Then $h(x) = x - \beta$ for some $\beta \in \mathbb{Q}$, then $f(x)$ has a rational root. By the above corollary, $f(x)$ has an integer root α and $\alpha \mid 1$, so $\alpha = \pm 1$.

But $f(1) = -3 = f(-1) \Rightarrow f(x)$ has no rational root.

Case 2: If $\deg(h(x)) = \deg(g(x)) = 2$. Then by Gauss's lemma, $f(x) = (x^2 + ax + b)(x^2 + cx + d)$, for some $a, b, c, d \in \mathbb{Z}$.

Then $f(x) = x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd$

$$= x^4 + (a+c)x^3 + (b+d+ac)x^2 + (bc+ad)x + bd.$$

Now comparing coefficients,

$$\begin{cases} a+c=0 \\ b+d+ac=-5 \\ bc+ad=0 \\ bd=1 \end{cases} \Rightarrow b=d=1 \text{ or } b=d=-1.$$

Then if $b=d=1$, $2+ac=-5$ and $a=-c$ and therefore

$$2-a^2=-5 \Rightarrow a^2=7 \Rightarrow a=\pm\sqrt{7} \notin \mathbb{Z},$$

and when $b=d=-1$, $-2+ac=-5$ and $a=-c$, then

$$-2-a^2=-5 \Rightarrow a^2=3 \Rightarrow a=\pm\sqrt{3} \notin \mathbb{Z},$$

therefore, Case 2 cannot happen. From both cases, we have that $f(x)$ is irreducible over $\mathbb{Q}$.

Einstein's Criterion

Example: Show that for prime p and $n \geq 1$, x^n+p is irreducible in $\mathbb{Q}[x]$.

By Gauss's Lemma, it is sufficient to show that there are no $g(x), h(x) \in \mathbb{Z}[x]$ such that $x^n+p=g(x)h(x)$ and $1 \leq \deg(g(x)), \deg(h(x)) \leq n-1$. Suppose

$$x^n+p=(b_r x^r+b_{r-1}x^{r-1}+\cdots+b_0)(c_s x^s+c_{s-1}x^{s-1}+\cdots+c_0)$$

We compare the coefficients for x^j as follows.

$$x^j=\begin{cases} p=b_0c_0 & \text{if } j=0. \quad (1) \Rightarrow p \mid a_0, p^2 \nmid a_0 \\ 0=b_j c_0+b_{j-1}c_1+\cdots+b_0c_j & \text{if } 1 \leq j \leq n-1 \quad (2) \Rightarrow p \mid a_1, \ldots, p \mid a_{n-1} \\ 1=b_j c_s & \text{if } j=n. \quad (3) \Rightarrow p \nmid a_n. \end{cases}$$

For (1) WLOG, say that $p \nmid b_0$ and $p \mid c_0$. Then by (3) note that $p \nmid b_r$ and $p \nmid c_s$. But if $p \mid c_0$ and $p \nmid c_s$. Let m be the smallest index such that $p \mid c_0, p \mid c_1, \ldots, p \mid c_{m-1}$ but $p \nmid c_m$. The

coefficient of x^m of the right hand side of

$$x = \underbrace{b_m c_0}_{p \mid c_0} + \underbrace{b_{m-1} c_1}_{p \mid c_1} + \cdots + \underbrace{b_1 c_{m-1}}_{p \mid c_{m-1}} + \underbrace{b_0 c_m}_{p \nmid c_m}$$

Then $m = n$ and $n = s$, so then

$\deg(c_s x^s + \cdots + c_0) = n$ and $\deg(b_r x^r + \cdots + b_0) = 0$

Therefore, $x^n + p$ is irreducible over $\mathbb{Q}$.

Theorem: Let p be a prime and $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. If $p \nmid a_n$ and $p \mid a_k$ for $1 \le k \le n-1$, and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Example: Let p be prime. Show that the p^{th} cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.

Proof: By the geometric series, observe that

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1) \quad (1)$$

and also note $\Phi_p(x)$ is reducible if and only if $\Phi_p(x+1)$ is reducible. Then

$$x\left((x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1) + 1\right) = (x+1)^p - 1$$

$$\Rightarrow x\,\Phi_p(x+1) = x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x + 1 - 1$$

$$= x\left(x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{2}x + p\right)$$

$$\Rightarrow \Phi_p(x+1) = \underbrace{x^{p-1}}_{a_{p-1}=1} + \underbrace{p x^{p-2}}_{a_{p-2}=p} + \cdots + \underbrace{\binom{p}{2}x}_{a_1=\binom{p}{2}} + \underbrace{p}_{a_0=p}.$$

By Einstein's Criterion, $\Phi_p(x+1)$ is irreducible, and thus, so is $\Phi_p(x)$.

Example: Show that $\mathbb{Q}(\sqrt{3}i) = \{a + b\sqrt{3}i : a, b \in \mathbb{Q}, i^2 = -1\}$ is a field.

Method 1: Show that the axioms for rings and then check that $\mathbb{Q}(\sqrt{3}i)$ is a commutative Division ring.

Method 2: Let $x = \sqrt{3}i \Rightarrow x^2 = -3 \Rightarrow x^2 + 3 = 0$ (a polynomial of the lowest degree that has $\sqrt{3}i$ as root.)

Also, $x^2 + 3$ is irreducible over $\mathbb{Q}$. Then $\mathbb{Q}[x]/\langle x^2+3\rangle$ is a field because $\mathbb{Q}[x]/\langle x^2+3\rangle$ is a field. (isomorphic to $\mathbb{Q}[\sqrt{3}i]$).

Now we show that $\mathbb{Q}[x]/\langle x^2+3\rangle \simeq \mathbb{Q}(\sqrt{3}i)$ using the first isomorphism for rings. Define $\phi: \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{3}i)$ by $\phi(f(x)) = f(\sqrt{3}i)$. Then $\ker(\phi) = \{r(x)(x^2+3) : r(x) \in \mathbb{Q}[x]\}$ because $\ker(\phi) = \langle x^2+3\rangle$.

We now check that ϕ is onto. For $a + b\sqrt{3}i \in \mathbb{Q}(\sqrt{3}i)$ $\phi(a+bx) = a + b\sqrt{3}i$. Then by 1st isomorphism theorem $\mathbb{Q}[x]/\langle x^2+3\rangle \cong \phi(\mathbb{Q}[x]) = \mathbb{Q}(\sqrt{3}i)$.