Irreducible Polynomials

Gauss's Lemma Suppose $f \in \mathbb{Z}[x]$ nonconstant and $f = gh$ where $g, h \in \mathbb{Q}[x]$. Then $\exists \delta \in \mathbb{Q}^\times$ s.t. $\tilde{g} = \delta g$, $\tilde{h} = \delta^{-1} h \in \mathbb{Z}[x]$ (and thus $f = \tilde{g}\tilde{h}$ in $\mathbb{Z}[x]$).

Pf p.529 □

Cor If $f \in \mathbb{Z}[x]$ has positive degree and is reducible over $\mathbb{Q}$, then $f = gh$ where $g, h \in \mathbb{Z}[x]$ have degrees $< \deg(f)$. □

Algorithm for irreducibility of $f \in \mathbb{Z}[x]$:

- WLOG, assume $f(0), f(1), \dots, f(n-1) \neq 0$.
- Fix integer $0 < d \leq n$.
- Fix divisors $a_0, \dots, a_d \in \mathbb{Z}$ of $f(0), \dots, f(d) \in \mathbb{Z}$.
- Construct $g \in \mathbb{Q}[x]$ of degree $\leq d$ s.t. $g(i) = a_i$ for $i = 0, \dots, d$ (Lagrange interpolation)
- Accept g if it has degree d and integer coeffs; reject it o/w.
- ~~Get~~ Do this for all $0 < d \leq n$, $a_0 \mid f(0), \dots, a_d \mid f(d)$ to get a set of "accepted" $g \in \mathbb{Z}[x]$.

Prop This set is finite, and f is irred/$\mathbb{Q}$ iff it is not divisible by any of the polynomials in this set.

Pf Each $f(i)$ has finitely many divisors, and g is uniquely determined by $a_0, \dots, a_d$, so we get only finitely many g this way. Remains to show f reducible iff some accepted g divides f.

($\Leftarrow$) ✓.

($\Rightarrow$) By the corollary, $f = gh$ where $g, h \in \mathbb{Z}[x]$, g has degree d, $0 < d \leq n$. For $0 \leq i \leq d$, set $a_i = g(i) \mid f(i)$. Lagrange interpolation gives $\tilde{g} \in \mathbb{Q}[x]$ with $\deg(\tilde{g}) \leq d$, $\tilde{g}(i) = a_i$. Then $\deg(g - \tilde{g}) \leq d$ and $(g - \tilde{g})(i) = 0$ for $0 \leq i \leq d$ ($d+1$ roots) so $g - \tilde{g} = 0 \Rightarrow g = \tilde{g}$ is in our list. □

Thm [Eisenstein criterion] Let $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, $a_n \neq 0$, $n > 0$. If there is a prime p s.t. $p \nmid a_n$, $p \mid a_{n-1}, \ldots, p \mid a_0$, and $p^2 \nmid a_0$, then f is irreducible over $\mathbb{Q}$.

Pf Suppose for $\not\subset$ f is of the above form & reducible over $\mathbb{Q}$. Then $f = gh$ for $g, h \in \mathbb{Z}[x]$ of degree $< n$. Write $\bar{\ } : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ for the mod p reduction map. Then $\bar{a}_n x^n = \bar{g}\bar{h}$ $\Rightarrow \bar{g} = \bar{a} x^r$, $\bar{h} = \bar{b} x^s$ for $\bar{a}\bar{b} = \bar{a}_n$, $r + s = n$.

TPS ~~Why~~ Why does $p \nmid a_n$ imply $r > 0, s > 0$?

Then $\bar{g} = \bar{a} x^r$ for $r > 0 \Rightarrow$ p divides constant term of g, and similarly for $h \Rightarrow p^2 \mid a_0$ $\not\subset$. $\square$

e.g. $x^n + px + p$, $n \geq 2$, p prime irred $/\mathbb{Q}$

Prop $\Phi_p := x^{p-1} + x^{p-2} + \cdots + 1$, p prime is irred $/\mathbb{Q}$.

Pf $\Phi_p(x+1) = \dfrac{(x+1)^p - 1}{x}$ and $(x+1)^p = x^p + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{p-1} x + 1$

so $\Phi_p(x+1) = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-1}$. By prime divisibility property of binomial coeffs, this satisfies the Eisenstein criterion, so $\Phi_p(x+1)$ is irred. Then reducibility of $\Phi_p(x)$ would contradict this. $\square$

Prop For p prime, $f = x^p - a \in F[x]$ is irred $/F$ iff f has no roots in F.

Pf ($\Rightarrow$) ✓.

($\Leftarrow$) Assume f reducible. Take L/F for which f splits completely $f = (x - \alpha_1) \cdots (x - \alpha_p)$, $\alpha_i \in L$. WLOG, $\alpha_1 \neq 0$. Set $\zeta_i = \dfrac{\alpha_i}{\alpha_1}$, $1 \leq i \leq p$. Then $\alpha_i^p \Rightarrow \zeta_i^p = 1$, so $\alpha_i = \zeta_i \alpha_1$ with ζ_i a pth root of unity: $f = (x - \zeta_1 \alpha_1)(x - \zeta_2 \alpha_1) \cdots (x - \zeta_p \alpha_1)$.

Suppose $f = gh$, $g, h \in F[x]$ monic with degrees $r, s < p$.

By unique fact'n + relabeling, $g = (x-\zeta_1\alpha_1)\cdots(x-\zeta_r\alpha_r)$.
Since the constant term of g is in F, $\underbrace{\zeta_1\cdots\zeta_r}_{\zeta}\alpha_1^r \in F$.

Note $\zeta^p = 1$.

Since $0<r<p$, p prime, $\exists m,n\in\mathbb{Z}$ s.t. $mr+np=1$. Then
$\zeta^m\alpha_1 = \zeta^m\alpha_1^{mr+np} = \underbrace{(\zeta\alpha_1^r)^m}_{\in F}\underbrace{(\alpha_1^p)^n}_{a\in F} \in F$. Thus $(\zeta^m\alpha_1)^p = (\zeta^p)^m\alpha_1^p$
$= a \Rightarrow \zeta^m\alpha_1$ is a root of $f = x^p - a$ lying in F. $\square$