Factorization in Polynomial Rings

Recall

F a field $\Rightarrow$ $F[x]$ UFD

$F[x]^* = F^* = F \setminus \{0_F\}$

$f(x), g(x) \neq 0_{F[x]} \Rightarrow \deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

Definition

$f \in F[x] \setminus \{0_{F[x]}\}$ monic if leading coefficient is 1_F

Observation

If $f(x), g(x) \in F[x] \setminus \{0_{F[x]}\}$ monic then

$f(x)$ and $g(x)$ associated $\Leftrightarrow f(x) = g(x)$

say $f(x)$ linear

Proposition $\deg(f(x)) = 1 \Rightarrow f(x)$ irreducible in $F[x]$

WLOG

Proof $f(x) = g(x)h(x) \Rightarrow \deg(g(x)) = 1,\ \deg(h(x)) = 0$

$\Rightarrow h(x) \in F[x]^* \Rightarrow f(x)$ irreducible $\square$

Theorem Given $f(x) \in F[x] \setminus \{0_{F[x]}\}$, $\alpha \in F$

say α is a root in F in $F[x]$

$f(\alpha) = 0_F \Leftrightarrow (x - \alpha) \mid f(x)$

Proof

$F[x]$

$(\Leftarrow)$ $f(x) = g(x)(x - \alpha) \Rightarrow f(\alpha) = g(\alpha)(\alpha - \alpha) = 0_F$

$(\Rightarrow)$ Assume $(x - \alpha) \nmid f(x)$

$\Rightarrow f(x) = q(x)(x-\alpha) + r$ ← degree 0 where $r \neq 0_F$

$\Rightarrow f(\alpha) = q(\alpha)(\alpha-\alpha) + r = r \neq 0_F$

$\square$

<u>Theorem</u> If $\deg(f(x)) = n$ and $\alpha_1, \ldots, \alpha_k \in F$ are distinct roots then $(x-\alpha_1)\ldots(x-\alpha_k) \mid f(x)$.
Hence $f(x)$ has at most n distinct roots in F.

<u>Proof</u>

$\alpha_i \neq \alpha_j$ $(i \neq j)$ $\Rightarrow x-\alpha_i \neq x-\alpha_j \Rightarrow$ $x-\alpha_i, x-\alpha_j$ are non-associate irreducibles

$f(\alpha_i) = 0_F \Rightarrow (x-\alpha_i) \mid f(x)$

$F[x]$ a UFD $\Rightarrow (x-\alpha_1)\ldots(x-\alpha_k) \mid f(x)$

$\square$

<u>Theorem</u>

Every non-constant $f(x) \in F[x]$ has a root in F $\iff$ Every irreducible in $F[x]$ is linear

<u>Proof</u>

$(\Rightarrow)$

Let $f(x)$ be irreducible in $F[x] \Rightarrow \deg(f(x)) \geq 1$

$\Rightarrow \exists\, \alpha \in F$ such that $f(\alpha) = 0_F \Rightarrow f(x) = (x-\alpha)g(x)$ ~~for~~ $F[x]^*$

$\Rightarrow g(x) \in (F[x])^* \Rightarrow \deg(f(x)) = 1$

$(\Leftarrow)$ $\deg(f(x)) \geq 1 \Rightarrow f(x) \neq 0_{F[x]}$ and $f(x) \notin F[x]^*$

$F[x]$ a UFD $\Rightarrow$ $f(x) = a\prod_{i=1}^{n}(x-\alpha_i)$ ← irreducible factors

$\Rightarrow$ $f(\alpha_1) = 0_F$

$\square$

<u>Definition</u>

F is <u>algebraically closed</u> $\Leftrightarrow$ Every non-constant $f(x) \in F[x]$ has a root in F

<u>Fundamental Theorem of Algebra</u>

$\mathbb{C}$ is algebraically closed

<u>Proof</u> Hard. Most straightforward proof uses complex analysis

$\square$

<u>Remarks</u>

$\mathbb{Q}$, $\mathbb{R}$, $\underset{\mathbb{F}_p}{\overset{\parallel}{\mathbb{Z}/p\mathbb{Z}}}$ are <u>not</u> algebraically closed

x^2+1 $\quad$ x^2+1 $\quad$ $x^p - x + 1$ ← None have a root in coefficient field

<u>Theorem</u> $f(x) \in \mathbb{R}[x]$ irreducible $\Rightarrow$ $\deg(f(x)) = 1$ or 2

<u>Proof</u>

Assume $f(x) \in \mathbb{R}[x]$ irreducible and $\deg(f(x)) > 2$

$\Rightarrow$ $f(x) = \underset{\mathbb{R}}{\overset{}{a}}\prod_{i=1}^{n}(x - \alpha_i)$, $a \in \mathbb{R}$, $\alpha_i \in \mathbb{C}$

factorization in $\mathbb{C}[x]$

$f(x) \in \mathbb{R}[x] \Rightarrow f(x) = a \prod_{i=1}^{n} (x - \overline{\alpha}_i)$ ← complex conjugate

$\Rightarrow \alpha_i \in \mathbb{R}$ or $\alpha_i \in \mathbb{C} \setminus \mathbb{R}$ and $\exists\, j \in \{1, \dots, n\}$

such that $\overline{\alpha}_i = \alpha_j$. ($\Rightarrow \alpha_i, \alpha_j$ complex conjugate pair)

$(x - \alpha_i)(x - \overline{\alpha}_i) \in \mathbb{R}[x] \Rightarrow f(x)$ product of <u>linear</u>

and <u>quadratic</u> terms $\Rightarrow f(x)$ reducible. Contradiction $\square$

Q/ What about $\mathbb{Q}[x]$?

Let's first think about factorization in <u>$\mathbb{Z}[x]$</u>.

FTOA : $\mathbb{Z}$ a U.F.D.

<u>Definition</u> Let R be a U.F.D.

$f(x) = a_0 + a_1 x + \dots + a_n x^n \in R[x]$ is <u>primitive</u> if

1/ $\deg(f(x)) \geq 1$

2/ $u \mid a_i \;\; \forall\, i \in \{0, \dots, n\} \Rightarrow u \in R^*$

<u>Example</u> $3 + 6x + 7x^2 \in \mathbb{Z}[x]$

<u>Gauss' Lemma</u> Let R be a U.F.D.

$f(x), g(x) \in R[x]$ primitive $\Rightarrow f(x)g(x)$ primitive

<u>Proof</u>

$f(x), g(x)$ primitive $\Rightarrow \deg(f(x)), \deg(g(x)) \geq 1 \Rightarrow \deg(f(x)g(x)) \geq 1$

Let $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $g(x) = b_0 + \dots + b_m x^m$

with $a_n \neq 0_R$, $b_m \neq 0_R$

$\Rightarrow f(x)g(x) = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m}$

where $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0$

Assume $f(x)g(x)$ not primitive. R a U.F.D. $\Rightarrow \exists \pi \in R$ irreducible such that $\pi \mid c_k \;\; \forall k \in \{0, \ldots, n+m\}$

Choose r, s minimal such that $\pi \nmid a_r$ and $\pi \nmid b_s$

$\Downarrow$

$\pi \mid a_i \;\; \forall i < r$

$\pi \mid b_j \;\; \forall j < s$

$c_{r+s} = a_0 b_{r+s} + \cdots + a_{r+s} b_0$

$$\Rightarrow a_r b_s = \underset{\uparrow \, \pi \text{ divides}}{c_{r+s}} - \underset{\uparrow \, \pi \text{ divides}}{a_0 b_{r+s}} \cdots - \underset{\uparrow \, \pi \text{ divides}}{a_{r-1} b_{s+1}} - \underset{\uparrow \, \pi \text{ divides}}{a_{r+1} b_{s-1}} \cdots - \underset{\uparrow \, \pi \text{ divides}}{a_{r+s} b_0}$$

R U.F.D.

$\Rightarrow \pi \mid a_r b_s \Rightarrow \pi \mid a_r$ or $\pi \mid b_s$ Contradiction

$\Rightarrow f(x)g(x)$ primitive $\square$

Observation :

Let $F = \mathrm{Frac}(R)$, $f(x) \in F[x]$, $\deg(f(x)) \geq 1$

$\deg(f(x)) = \deg(f_0(x))$

$\Rightarrow f(x) = \frac{\alpha}{\beta} f_0(x)$ where $\frac{\alpha}{\beta} \in F$, $f_0 \in R[x]$ primitive

unique up to a unit in $R[x]$.

Example

$f(x) = \frac{2}{3} + \frac{4}{3}x + 2x^2 \in \mathbb{Q}[x]$

Primitive in $\mathbb{Z}[x]$

$\Rightarrow 3f(x) = 2 + 4x + 6x^2 = 2(1 + 2x + 3x^2)$

$\Rightarrow f(x) = \frac{2}{3}(1 + 2x + 3x^2)$

Theorem Let R be a U.F.D., $F = \mathrm{Frac}(R)$, $f(x) \in R[x] \subset F[x]$.

$f(x)$ irreducible in $R[x] \Rightarrow f(x)$ irreducible in $F[x]$.

Proof Prove Contrapositive:

$f(x)$ reducible in $F[x] \Rightarrow f(x)$ reducible in $R[x]$

Let $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x]$, $\deg(g(x)), \deg(h(x)) \geq 1$

$\notin R[x]^*$ $\notin R[x]^*$

Let
$$\left.\begin{aligned} f(x) &= \alpha f_0(x) \\ g(x) &= \frac{a}{b} g_0(x) \\ h(x) &= \frac{c}{d} h_0(x) \end{aligned}\right\} \quad f_0(x), g_0(x), h_0(x) \in R[x] \text{ primitive}$$

Primitive by Gauss' Lemma

$$\Rightarrow \alpha f_0(x) = \frac{ac}{bd}(g_0(x)h_0(x))$$

$$\Rightarrow f_0(x) = u\, g_0(x) h_0(x) \quad \text{where } u \in R^*$$

$$\Rightarrow f(x) = \alpha u\, g_0(x) h_0(x) \Rightarrow f(x) \text{ reducible in } R[x].$$

$\square$

Warning:

$f(x)$ irreducible in $F[x] \not\Rightarrow f(x)$ irreducible in $R[x]$

For example $2x + 6 = 2(x+3)$

Corollary If $f(x) \in R[x]$ monic and $\mu \in F$ a root in F, then $\mu \in R$.

Proof Let $\mu = \frac{a}{b}$, with 1_F an HCF of a and b.

$f(\frac{a}{b}) = 0 \Rightarrow f(x) = (x - \frac{a}{b})\, h(x)\ ,\ h(x) \in F[x]$

$x - \frac{a}{b} = \frac{1}{b}(bx - a)$ ← primitive in $R[x]$

By above proof $(bx-a) \mid f(x)$ ← in $R[x]$

$f(x)$ <u>monic</u> $\Rightarrow b \in R^* \Rightarrow \frac{a}{b} = \frac{ab^{-1}}{1} \Rightarrow \frac{a}{b} \in R$ □

<u>Eisensteins Criterion</u>

Let R be a U.F.D., $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$

$\deg(f(x)) \geq 1$

Assume $\exists\ \pi \in R$ irreducible such that

1/ $\pi \nmid a_n$

2/ $\pi \mid a_i \quad \forall i \in \{0, \dots, n-1\}$

3/ $\pi^2 \nmid a_0$

then $f(x)$ is irreducible in $F[x]$

<u>Proof</u>

Assume 1/, 2/, 3/ hold but $f(x)$ reducible in $F[x]$

$\Rightarrow f(x)$ reducible in $R[x]$ and $f(x) = g(x)h(x)$

with $g(x), h(x) \in R[x]$, $\deg(g(x)), \deg(h(x)) \geq 1$

Let $g(x) = b_0 + \dots + b_rx^r$ $\quad b_r \neq 0_R,\ c_s \neq 0_R$

$h(x) = c_0 + \dots + c_sx^s$ $\quad r+s = n,\ r,s \geq 1$

$r < n,\ s < n$

$a_0 = b_0 c_0$ WLOG

$\pi^2 \nmid a_0$, $\pi \mid a_0$ $\Rightarrow$ $\pi \mid b_0$ <u>and</u> $\pi \nmid c_0$ $\pi \mid b_j$ $\forall\, j < i$

$\pi \nmid a_n \Rightarrow$ $\pi \nmid b_r$ and $\pi \nmid c_s$

Choose $i \in \{1, \dots r\}$ <u>minimal</u> such that $\pi \nmid b_i$

$$a_i = b_i c_0 + b_{i-1} c_1 + \dots + b_0 c_i$$

$$\Rightarrow b_i c_0 = \underbrace{a_i}_{\pi \text{ divides}} - \underbrace{b_{i-1} c_1}_{\pi \text{ divides}} - \dots - \underbrace{b_0 c_i}_{\pi \text{ divides}}$$

$\Rightarrow \pi \mid b_i c_0$

But $\pi \nmid c_0 \Rightarrow \pi \mid b_i$ <u>Contradiction</u>.

$\Rightarrow f(x)$ irreducible in $F[x]$.

<u>Corollary</u> In $\mathbb{Q}[x]$ there are irreducible polynomials of any degree.

<u>Proof</u>

$\mathbb{Z}$ a UFD. $\mathbb{Q} = \text{Frac}(\mathbb{Z})$

Eisensteins criterion $\Rightarrow$ $2 + 2x + \dots + 2x^{n-1} + x^n$ is irreducible in $\mathbb{Q}[x]$ $\forall n \in \mathbb{N}$

$\square$