Section 9.4 Irreducibility Criteria

Recall: $p(x) \in R[x]$ is irreducible if $p(x) \neq 0$ and whenever $p(x) = a(x)b(x)$, one of $a(x)$ or $b(x)$ is a unit. If R is ~~an~~ field $f(x)$ being irreducible means it can't be factored into two polynomials of lower degree.

Ex $p(x) = x^2+1$ irreducible in $\mathbb{R}[x]$, reducible in $\mathbb{C}[x]$, what about $\mathbb{Z}_2[x]$?

Deciding whether or not a polynomial is irreducible is a tricky business. We now develop some criteria for this.

Proposition 9 Let $p(x) \in F[x]$ where F is a field. Then $p(x) = (x-a)g(x) \iff p(a) = 0$

Example Is $p(x) = 1 + 3x + 4x^2 + x^3 + x^4 + 2x^5 + 3x^6$ irreducible in $\mathbb{Z}_5[x]$? No because $p(1) = 0$

we know $p(x) = (x-1)g(x) = (x+4)g(x)$

[can find $g(x)$ with long division].

Strategy To see if $p(x)$ factors with a linear term (in a finite field) ~~Just check~~ find roots a of $p(x)$. Then we know $p(x) = (x-a)g(x)$.

But checking for zeros doesn't guarantee an answer.

Does $f(x) = x^4 + 2x^2 + 1$ factor over $\mathbb{Z}_3[x]$?

$$\left.\begin{array}{l} f(0)=1 \\ f(1)=1 \\ f(2)=1 \end{array}\right\}$$ Doesn't factor with a linear term, but $x^4+2x^2+1 = (x^2+1)(x^2+1)$

Proposition 10 A polynomial of degree 2 or 3 over a field F is reducible $\iff$ it has a root in F

Example Is x^2+2x+1 reducible over $\mathbb{Z}_3$?

$f(0)=1$
$f(1)=1$
$f(2)=0$ $\longrightarrow$ $x^2+2x+1 = (x-2)(x-2) = (x+1)(x+1)$

Observation: Suppose $f(x) = a_0 + a_1 x + \cdots + x^n \in \mathbb{Z}[x]$ (monic)
If $f(a)=0$, some $a \in \mathbb{Z}$, then $a \mid a_0$
Reason $f(a)=0 \Rightarrow f(x) = (x-a)(x^{n-1} + \cdots + b)$ $\quad ab = a_0$

Example $f(x) = x^4 + 5x^3 + 5x^2 - 5x - 6$ $\quad$ possibilities for roots: $\pm 1, \pm 2, \pm 3, \pm 6$

Test $f(1)=0$
$f(-1)=0$
$f(2)\neq 0$
$f(-2)=0$
$f(-3)=0$

$$f(x) = (x-1)(x+1)(x+2)(x+3)$$

Proposition 11 Suppose $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$.
If $f(\frac{r}{s}) = 0$ then $r \mid a_0$ and $s \mid a_n$.

Proposition 12 Suppose $I \subseteq R$ is a proper ideal, $p(x) \in R[x]$ monic.
If $p(x)$ factors in $R[x]$, Then ~~it fact~~ $\overline{p(x)}$ factors in $R/I\,[x]$.
i.e. If $p(x)$ irreducible in $R/I\,[x]$, Then its irreducible in $R[x]$.

Corollary 13 (Eisenstein's Criterion for $\mathbb{Z}[x]$)
Suppose $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, and p is prime.
Then $f(x)$ is $\underbrace{\text{irreducible}}_{\text{in } \mathbb{Z}[x] \text{ and } \mathbb{Q}[x]}$ if $p \mid a_i$ $\forall_i$ but $p^2 \nmid a_0$

Example: $$f(x) = x^{10} - 25x^3 + 10x^2 - 30$$

$5 \mid 25 \qquad 5 \mid 10 \qquad 5 \mid 30$, $\; 5^2 \nmid 30$

Thus $f(x)$ is irreducible in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$.

Section 9.5 Polynomial Rings over Fields II

Proposition 15 Suppose F is a field. Then:
$\mathbb{R}[x]/(f(x))$ is a field $\Leftrightarrow$ $f(x)$ is irreducible.
i.e. $(f(x))$ is a maximal ideal $\Leftrightarrow$ $f(x)$ is irreducible

Proof $\mathbb{R}[x]/(f(x))$ is a field $\overset{\text{Ch 7, Prop 12}}{\Longleftrightarrow}$ $(f(x))$ is maximal

$\overset{\text{Ch. 8 Prop 7}}{\Longleftrightarrow}$ $(f(x))$ is prime

$\overset{\text{Def of prime}}{\Longleftrightarrow}$ $f(x)$ is prime

$\overset{\text{Ch 8 Prop 12}}{\Longleftrightarrow}$ $f(x)$ is irreducible $\blacksquare$

Example x^2+1 is irreducible in $\mathbb{R}[x]$, and $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

Example A field with 9 elements.

Note $f(x) = x^2+1$ is irreducible in $\mathbb{Z}/3\mathbb{Z}$ $\begin{cases} f(0) = 1 \\ f(1) = 2 \\ f(2) = 2 \end{cases}$

Thus $\mathbb{Z}/3\mathbb{Z}[x]/(x^2+1) = F$ is a field.

$F = \{a + bx \mid a, b \in \mathbb{Z}/3\mathbb{Z}\}$, so $|F| = 9$.

Addition: $(a+bx)+(c+dx) = (a+c) + (b+d)x$

Multiplication: $(a+bx)(c+dx) = (ac-bd) + (ad+bc)x$

$$(a+bx)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}x$$

Reason $(a+bx)\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}x\right)$

$$= \frac{a^2+b^2}{a^2+b^2} + 0x = \underline{1}.$$

Proposition 16 Suppose $g(x) \in F[x]$ is monic, and

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$$

be its prime factorization. Then

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times \cdots \times F[x]/(f_k(x)^{n_k}).$$

Example

$$\mathbb{R}[x]/(x^2-1) \cong \mathbb{R}[x]/(x+1) \times \mathbb{R}[x]/(x-1)$$
$$\cong \mathbb{R} \times \mathbb{R}$$

(not a field.)