1.7 Lecture 7: Irreducible polynomials

Let $\mathbb{F}$ be a field.

- The **group of units of** $\mathbb{F}$ is

$$\mathbb{F}^\times = \{a \in \mathbb{F} \mid \text{there eixsts } c \in \mathbb{F} \text{ with } ca = ac = 1\}$$

- The **group of units of** $\mathbb{F}[x]$ is

$$\mathbb{F}[x]^\times = \{f(x) \in \mathbb{F}[x] \mid \text{there eixsts } g(x) \in \mathbb{F}[]x] \text{ with } g(x)f(x) = f(x)g(x) = 1.\}$$

HW:. Show that $\mathbb{F}^\times = \{a \in \mathbb{F} \mid a \neq 0\}$.

HW:. Show that $\mathbb{F}[x]^\times = \mathbb{F}^\times$.

Let $f(x) \in \mathbb{F}[x]$.

- The polynomial $f(x)$ is **irreducible** if
  (a) $f(x) \neq 0$,
  (b) $f(x) \in \mathbb{F}[x]^\times$,
  (c) There do not exist $g(x), h(x) \in \mathbb{F}[x]$ such that $g(x)h(x) = f(x)$ and $g(x) \notin \mathbb{F}[x]^\times$ and $h(x) \notin \mathbb{F}[x]^\times$.

- The **ideal generated by** $f(x)$ is

$$f(x)\mathbb{F}[x] = \{f(x)g(x) \mid g(x) \in \mathbb{F}[x]\}.$$

- The ideal $f(x)\mathbb{F}[x]$ is **a maximal ideal** if there does not exist $g(x) \in \mathbb{F}[x]$ such that

$$f(x)\mathbb{F}[x] \subsetneq g(x)\mathbb{F}[x] \subsetneq \mathbb{F}[x].$$

Proposition 1.14. *Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$. The following are equivalent*

(a) $f(x)$ is irreducible in $\mathbb{F}[x]$, *(b) $f(x)\mathbb{F}[x]$ is a maximal ideal,* *(c) $\frac{\mathbb{F}[x]}{f(x)\mathbb{F}[x]}$ is a field.*

1.7.1 Comparing polynomials in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Let $f(x) \in \mathbb{Z}[x]$. The polynomial

$$f(x) = c_0 + c_1 x + \cdots + c_\ell x^\ell \qquad \text{is } \textbf{primitive} \text{ if} \qquad \gcd(c_0, \ldots, c_\ell) = 1.$$

Proposition 1.15. *Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if*

either $f(x) = \pm p$, where p is a prime integer,
or $f(x)$ is a primitive polynomial and $f(x)$ is irreducible in $\mathbb{Q}[x]$.

1.7.2 Comparing polynomials in $\mathbb{Z}[x]$ and $\mathbb{F}_p[x]$

Proposition 1.16. *Let $f(x) \in \mathbb{Z}[x]$ and let $p \in \mathbb{Z}_{>0}$ be prime. Let $\overline{f(x)}$ denote the image of $f(x)$ in $\mathbb{F}_p[x]$.*

If $\deg(\overline{f(x)}) = \deg(f(x)$ and $\overline{f(x)}$ is irreducible in $\mathbb{F}_p[x]$

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