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 the set of multiples of $f(x)$,

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

- 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

$$f(x) = c_0 + c_1x + \cdots + c_\ell x^\ell \qquad \text{is **primitive** if} \qquad \gcd(c_0, \ldots, c_\ell) = 1.$$

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 $\mathbb{Z}[x]$.

1.7.3 Primitive polynomials and Eisenstein's criterion

The polynomial

$$f(x) = c_0 + c_1x + \cdots + c_\ell x^\ell \in \mathbb{Z}[x] \qquad \text{is } \textbf{primitive} \text{ if} \qquad \gcd(c_0, \ldots, c_\ell) = 1.$$

HW: Let $f(x) = c_0 + c_1x + \cdots + c_\ell x^\ell \in \mathbb{Z}[x]$. Show that $f(x)$ is primitive if and only if $f(x)$ satisfies:

$$\text{if } p \in \mathbb{Z}_{>0} \text{ and } p \text{ is prime then } \overline{f(x)} \neq 0 \text{ in } \mathbb{F}_p[x].$$

The **group of units of** $\mathbb{Z}$ is

$$\mathbb{Z}^\times = \{a \in \mathbb{Z} \mid \text{there exists } b \in \mathbb{Z} \text{ such that } ab = ba = 1\}.$$

HW: Show that $\mathbb{Z}^\times = \{-1, 1\}$.

Theorem 1.17. *Let* $f(x) \in \mathbb{Z}[x]$.

(a) There exist

$$c \in \mathbb{Q} \text{ and a primitive } g(x) \in \mathbb{Z}[x] \qquad \text{such that} \qquad f(x) = cg(x).$$

(b) If $g'(x) \in \mathbb{Z}[x]$ *is primitive and* $c' \in \mathbb{Q}$ *and* $f(x) = c'g'(x)$ *then there exists* $u \in \mathbb{Z}^\times$ *such that*

$$c' = u^{-1}c \qquad \text{and} \qquad g'(x) = ug(x).$$

(c) If $f(x)$ *is irreducible in* $\mathbb{Q}[x]$ *then* $g(x)$ *is irreducible in* $\mathbb{Q}[x]$.

Proposition 1.18. *(Eisenstein criterion) Let* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ *and let* $p \in \mathbb{Z}_{>0}$ *be a prime integer. Assume*

(a) p *does not divide* a_n,

(b) p *divides each of* $a_{n-1}, a_{n-2}, \ldots, a_0$,

(c) p^2 *does not divide* a_0,

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

Proof. Assume $p \in \mathbb{Z}_{>0}$ with p prime and $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$.
Assume p does not divide a_n and p divides each of $a_{n-1}, \ldots, a_0$.
To show: If p^2 does not divide a_0 then $f(x)$ is irreducible in $\mathbb{Z}[x]$.
To show: If $f(x)$ is reducible in $\mathbb{Z}[x]$ then p^2 divides a_0.
Assume $f(x)$ is reducible in $\mathbb{Z}[x]$.
Then there exists $g(x), h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$ (and $g(x), h(x) \notin \{0, 1, -1\}$).
Write $g(x) = g_kx^k + \cdots + g_0$ and $h(x) = h_\ell x^\ell + \cdots + h_0$.
Letting $\bar{a} = a \bmod p$ for $a \in \mathbb{Z}$, then

$$\overline{a_n}x^n = \overline{a_n}x^n + \cdots + \overline{a_0} = \overline{f(x)} = \overline{g(x)h(x)} = (\overline{g_k}x^k + \cdots + \overline{g_0})(\overline{h_\ell}x^\ell + \cdots + \overline{h_0}). \tag{1.1}$$

Since the only factorization of $\overline{a_n}x^n$ in $\mathbb{F}_p[x]$ of the form (1.1) is $\overline{a_n}x^n = \overline{g_k}\,\overline{h_\ell}x^{k+\ell} = (\overline{g_k}x^k)(\overline{h_\ell}x^\ell)$ then

$$\overline{g_{k-1}} = \cdots \overline{g_0} = \overline{h_{\ell-1}} = \cdots = \overline{h_0} = 0.$$

So both g_0 and h_0 are divisible by p.
Using the fact that $\mathbb{Z}$ is a unique factorization domain then $a_0 = g_0h_0$ is divisible by p^2. □