11.03.2024 ①
Algebra Lect. 7
A. Ram

Irreducible polynomials

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

The <u>group of units of $\mathbb{F}[x]$</u> is

$$\mathbb{F}[x]^\times = \left\{ a(x) \in \mathbb{F}[x] \;\middle|\; \begin{array}{l} \text{there exists } b(x) \in \mathbb{F}[x] \\ \text{with } a(x)b(x) = 1 \end{array} \right\}$$

<u>HW</u>: Use $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$ to show that $\mathbb{F}[x]^\times = \mathbb{F}^\times$.

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

The polynomial $f(x)$ is <u>irreducible in $\mathbb{F}[x]$</u> if $f(x)$ satisfies:

(a) $f(x) \neq 0$ and $f(x) \notin \mathbb{F}[x]^\times$

(b) There do not exist $g(x), h(x) \in \mathbb{F}[x]$ such that

(ba) $g(x), h(x) \notin \mathbb{F}[x]^\times$

(bb) $f(x) = g(x)h(x)$.

Let

$$\mathbb{F}[x]_{\text{monic}} = \left\{ x^\ell + c_{\ell-1}x^{\ell-1} + \cdots + c_1 x + c_0 \;\middle|\; \begin{array}{l} \ell \in \mathbb{Z}_{\geq 0} \\ c_0, \ldots, c_{\ell-1} \in \mathbb{F} \end{array} \right\}$$

Examples

(1) Let $f(x) \in \mathbb{C}[x]_{\text{monic}}$. Then $f(x)$ is irreducible in $\mathbb{C}[x]$ if and only if

$$f(x) = x - \alpha \quad \text{with } \alpha \in \mathbb{C}.$$

(2) Let $f(x) \in \mathbb{R}[x]_{\text{monic}}$.
If $\alpha \in \mathbb{C}$ is a root of $f(x)$
then $\bar{\alpha} \in \mathbb{C}$ is a root of $f(x)$.

So $f(x)$ is irreducible in $\mathbb{R}[x]$ if and only if

$$f(x) = x - \alpha \quad \text{with } \alpha \in \mathbb{R}$$

OR

$$f(x) = x^2 + bx + c \quad \text{with } b^2 - 4c \in \mathbb{R}_{<0}.$$

(3) Let $f(x) \in \mathbb{Q}[x]_{\text{monic}}$.

Step 1: Make a common denominator.

$$f(x) = \frac{1}{d} g(x) \quad \text{with } g(x) \in \mathbb{Z}[x].$$

Step 2: Pull out common factors.

$$f(x) = \frac{c}{d} h(x) \quad \text{with } h(x) \in \mathbb{Z}[x] \text{ primitive}.$$

Step 3: If there exists $p \in \mathbb{Z}_{>0}$ with p prime such that

$\overline{h(x)} = (h(x) \bmod p)$ is irreducible in $\mathbb{F}_p[x]$

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

and $f(x)$ is <u>irreducible</u> in $\mathbb{Q}[x]$.

Let $h(x) = h_k x^k + \cdots + h_1 x + h_0 \in \mathbb{Z}[x]$.

The polynomial $h(x)$ is <u>primitive</u> if

$$\gcd(h_0, h_1, \ldots, h_k) = 1.$$

<u>Example</u> $f(x) = x^3 + \frac{7}{5}x^2 + \frac{1}{8}x + \frac{3}{8} \in \mathbb{Q}[x]_{\text{monic}}$

Then $f(x) = \frac{1}{40}(40x^3 + 28x^2 + 5x + 15) = \frac{1}{20}h(x)$

$$\overline{h(x)} = 5x^3 + 0x^2 + 5x + 1 \text{ in } \mathbb{F}_7[x].$$

Since $\overline{h(x)}$ has no root in $\mathbb{F}_7[x]$

then $\overline{h(x)}$ has no factor $x - \alpha$ with $\alpha \in \mathbb{F}_7$.

So $\overline{h(x)}$ is irreducible in $\mathbb{F}_7[x]$.

So $h(x)$ is irreducible in $\mathbb{Z}[x]$

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

$\mathbb{A}$-modules and ideals

Let $\mathbb{A} = \mathbb{F}[x]$. An $\mathbb{A}$-module is a set V with two functions

$$\begin{matrix} V \times V \to V \\ (v_1, v_2) \mapsto v_1 + v_2 \end{matrix} \quad \text{and} \quad \begin{matrix} \mathbb{A} \times V \to V \\ (c, v) \mapsto cv \end{matrix}$$

such that

same axioms as for vector spaces.

Let V be an $\mathbb{A}$-module.

An $\mathbb{A}$-submodule of V is a subset $W \subseteq V$ such that

(a) $0 \in W$,

(b) If $w_1, w_2 \in W$ then $w_1 + w_2 \in W$,

(c) If $c \in \mathbb{A}$ and $w \in W$ then $cw \in W$.

Example $V = \mathbb{A}$ is an $\mathbb{A}$-module with

$$\begin{matrix} V \times V \to V \\ (a_1, a_2) \mapsto a_1 + a_2 \end{matrix} \quad \text{and} \quad \begin{matrix} \mathbb{A} \times V \to V \\ (c, a) \mapsto ca. \end{matrix}$$

An ideal of $\mathbb{A}$ is an $\mathbb{A}$-submodule of $\mathbb{A}$.

Example Let $\mathbb{A} = \mathbb{F}[x]$.
Let $f(x) \in \mathbb{A}$. Then

$$f(x)\mathbb{F}[x] = \{f(x)g(x) \mid g(x) \in \mathbb{F}[x]\}$$
$$= f\mathbb{A} = \{cf \mid c \in \mathbb{A}\}$$
$$= \mathbb{A}\text{-span}\{f\}$$

is an ideal of $\mathbb{A}$.

The ideal $f\mathbb{A}$ is a maximal ideal of $\mathbb{A}$
if (a) $f\mathbb{A} \neq \mathbb{A}$ and
(b) there does not exist $g(x) \in \mathbb{A}$ with
$$f\mathbb{A} \subsetneq g\mathbb{A} \subsetneq \mathbb{A}.$$

Theorem Let $\mathbb{A} = \mathbb{F}[x]$ and $f \in \mathbb{A}$.
The following are equivalent:

(a) f is irreducible in $\mathbb{F}[x]$,

(b) $f\mathbb{A}$ is a maximal ideal,

(c) $\dfrac{\mathbb{A}}{f\mathbb{A}} = \dfrac{\mathbb{F}[x]}{f(x)\mathbb{F}[x]}$ is a field.