Primitive polynomials

Let R be a UFD.

A polynomial $f(x) = c_0 + c_1 x + \cdots + c_k x^k$ in $R[x]$ is <u>primitive</u> if

$$\gcd(c_0, c_1, \ldots, c_k) = 1.$$

Proposition Let R be a UFD.

Let $\mathbb{F} = \mathrm{Frac}(R)$ and let $f(x) \in \mathbb{F}[x]$.

(a) There exists $c \in \mathbb{F}$ and a primitive polynomial $g(x) \in R[x]$ such that

$$f(x) = c\, g(x).$$

(b) The factors c and $g(x)$ are unique up to multiplication by a unit in R, i.e. If

$$f(x) = C\, G(x), \text{ with } C \in \mathbb{F} \text{ and}$$

$G(x) \in R[x]$ primitive then there exists $u \in R^\times$ such that $C = u^{-1} c$ and $G(x) = u\, g(x)$.

(c) $f(x)$ is irreducible in $\mathbb{F}[x]$ if and only if $g(x)$ is irreducible in $R[x]$.

Sketch of Proof $\Rightarrow$: (<) Proof by contrapositive.

20.05.2024 (2)

Algebra Lect 34

A. Rau

Assume $g(x)$ is not irreducible in $R[x]$.

Then there exist $g_1(x)$ and $g_2(x)$ in $R[x]$ such that

$$g(x) = g_1(x)\,g_2(x) \quad \text{and} \quad g_1(x), g_2(x) \notin R[x]^\times.$$

So $f(x) = c\,g(x) = (c\,g_1(x))\cdot g_2(x)$ is a factorization in $\mathbb{F}[x]$.

So $f(x)$ is not irreducible in $\mathbb{F}[x]$.

(4) $\Leftarrow$: Proof by contrapositive.

Assume $f(x)$ is not irreducible in $\mathbb{F}[x]$

Then

$$f(x) = f_1(x) f_2(x) \quad \text{and} \quad f(x) = c\,g(x),$$

with $f_1(x), f_2(x) \notin \mathbb{F}[x]^\times$ and there exist $c_1, c_2 \in \mathbb{F}$ and $g_1(x), g_2(x)$ primitive in $R[x]$ such that $f_1(x) = c_1 g_1(x)$ and $f_2(x) = c_2 g_2(x)$.

So

$$f(x) = c_1 c_2\, g_1(x)\, g_2(x).$$

By Gauss' lemma $g_1(x) g_2(x)$ is primitive.

By uniqueness of primitive decomposition there is $u \in R^\times$ such that $g(x) = u\,g_1(x)\,g_2(x)$. //

20.05.2024
Algebra Lect 34 ③
A. Ram

<u>Proposition</u> Let R be a UFD.

(a) Let $g(x) \in R[x]$. Then $g(x)$ is not primitive if and only if there exists an irreducible $p \in R$ such that

$\pi_p(f(x)) = 0$, where $\pi_p : R[x] \longrightarrow \frac{R}{pR}[x]$
$$c_0 + \cdots + c_k x^k \mapsto \bar{c}_0 + \cdots + \bar{c}_k x^k$$
with $\bar{c} = c + pR$ is c mod pR.

(b) (Gauss' Lemma). Let $g_1(x), g_2(x) \in R[x]$ be primitive polynomials. Then
$g_1(x) g_2(x)$ is a primitive polynomial in $R[x]$.

<u>Proof</u> (b) Proof by contrapositive.
Assume $g_1(x) g_2(x)$ is not primitive.
To show: $g_1(x)$ is not primitive ~~or~~
$g_2(x)$ is not primitive.
To show: If $g_1(x)$ is primitive then
$g_2(x)$ is not primitive.
Assume $g_1(x)$ is primitive.
By (a), $\pi_p(g_1(x)) \neq 0$ and $\pi_p(g_1(x) g_2(x)) = 0$.
there exists an irreducible $p \in R$ such that

20.05.2024
Algebralect 34.
A. Ram.

4

So
$\pi_p(q_1(x)) \cdot \pi_p(q_2(x)) = 0$ and

$\pi_p(q_1(x)) \neq 0$.

Since $\frac{R}{pR}$ is an integral domain then
$\pi_p(q_2(x)) = 0$. (every irreducible element is prime)

So $q_2(x)$ is not primitive.

(a) $\Rightarrow$ Assume $f(x) = c_0 + c_1 x + \cdots + c_k x^k$ is not primitive.

Then there exists p irreducible in R such that p dividese $c_0, c_1, \ldots, c_k$.

So $c_0, c_1, \ldots, c_k \in pR$ and $\pi_p(c_0) = \cdots = \pi_p(c_k) = 0$.

So $\pi_p(f(x)) = 0$

$\Leftarrow$: Assume $p \in R$ is irreducible and
$\pi_p(f(x)) = 0$.

Then $\pi_p(c_0) = \cdots = \pi_p(c_k) = 0$.

So $c_0, \ldots, c_k \in pR$ and p divides $c_0, \ldots, c_k$.

So p divides $\gcd(c_0, \ldots, c_k)$ and
$f(x) = c_0 + c_1 x + \cdots + c_k x^k$ is not primitive.

20.05.2024 (5)
Algebra Lect. 34
A. Ram

Proposition Let R be a UFD.
Let $d \in R$ with $d \neq 0$ and $d \notin R^\times$.
Then
d is prime if and only if d is irreducible.

Proof $\Rightarrow$ Assume d is prime.
To show: d is irreducible.
To show: If $d = ab$ then $a \in R^\times$ or $b \in R^\times$.
Assume $d = ab$. ~~and $a \notin R^\times$.~~
~~To show: $b \in R^\times$~~
Since dR is a prime ideal and $ab \in dR$
then $a \in dR$ or $b \in dR$.
Case 1: $a \in dR$.
Then there exists $r \in R$ such that $a = dr$.
So $d = ab = drb$.
By cancellation, $1 = rb$. So $b \in R^\times$.
Case 2: $b \in dR$.
Then there exists $s \in R$ such that $b = ds$.
So $d = ab = das$.
By cancellation, $1 = as$. So $a \in R^\times$.
So $b \in R^\times$ or $a \in R^\times$.

$\Leftarrow$ Assume $d \in R$ is irreducible.

To show: dR is a prime ideal.

Assume $ab \in dR$.

To show: $a \in dR$ or $b \in dR$.

Assume $a \notin dR$. To show: $b \in dR$.

Let $p_1, \ldots, p_k \in R$ and $m_1, \ldots, m_k, n_1, \ldots, n_k, n_0 \in \mathbb{Z}_{\geq 0}$ with

$$a = d^0 p_1^{m_1} \cdots p_k^{m_k} \quad \text{and} \quad b = d^{n_0} p_1^{n_1} \cdots p_k^{n_k}.$$

Since

$$ab = d^{n_0} p_1^{m_1+n_1} \cdots p_k^{m_k} = dr$$

then $n_0 \geq 1$. So $b \in dR$.

So dR is a prime ideal. //.

Note that:

$$\mathbb{F}[x]^\times = \mathbb{F}^\times \quad \text{and} \quad R[x]^\times = R^\times,$$

since R is an integral domain.