R : Commutative ring

$\Downarrow$

$R[x]$: Commutative ring of polynomials with coefficients in R.

Example:

$R = \mathbb{Z}/4\mathbb{Z}$

$2x+1, \quad 2 \in \mathbb{Z}/4\mathbb{Z}[x]$

$$\begin{array}{cc} \parallel & \parallel \\ \Big[(1,2,0,\ldots), & (2,0,\ldots,0,\ldots)\Big] \end{array}$$

$(2x+1)\cdot 2 = 4x+2$

leading coefficient is not invertible

$= 2 \in (\mathbb{Z}/4\mathbb{Z})[x]$

$\deg(2x+1) = 1$ But $\deg((2x+1)\cdot 2) = 0$.

$\deg(2) = 0$

$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

is **not** always true.

Rmk: In a group G

$$g \cdot h = h$$

$\Rightarrow g = e$ is the identity

$$g \cdot h = h$$
$$\Rightarrow g \cdot h \cdot h^{-1} = e$$

This is not a contradiction of the example because 2 does not have a multiplicative inverse in $\mathbb{Z}/4\mathbb{Z}$.

Monic polynomials

Def^n $f(x) \in R[x] \setminus \{0\}$

$\deg(f(x)) = n \geq 0$

Then $f(x)$ is **monic** if the **leading coefficient** (i.e. the coefficient of x^n)

is invertible

Rmk: R: comm. ring
$x \in R$: invertible if x has
a multiplicative inverse

In $\mathbb{Z}/n\mathbb{Z}$ the invertible elements are in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Notation: $R^\times$: set of invertible elements in R

Rmk: This is an abelian group under multiplication

Example: · $x+1$ is monic

· $2x+1 \in \mathbb{Z}/4\mathbb{Z}[x]$ is not monic

· $2x+1 \in \mathbb{Z}/5\mathbb{Z}[x]$ is monic.

Rmk: Over a field, every non-zero polynomial is monic.

Division algorithm

Proposition: • $f(x) \in R[x]$ monic of deg ≥ 1

• $g(x) \in R[x]$

Then $\exists\, q(x) \in R[x]$, $r(x) \in R[x]$

s.t. (1) $g(x) = q(x) f(x) + r(x)$

(2) $\deg r(x) < \deg f(x)$

Moreover: $r(x)$ (the remainder) is uniquely determined

Pf: By induction on $\deg g(x)$.

• Base case ✓ If $\deg g(x) < \deg f(x)$
$g(x) = 0 \cdot f(x) + g(x)$

• Inductive step (assume $\deg g(x) \geq \deg f(x)$)

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$$
$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$

$a_n \in R^\times$

Look at

$$g_1(x) = g(x) - x^{m-n} \cdot a_n^{-1} b_m f(x)$$

$$\underbrace{x^{m-n}(a_n^{-1} b_m a_n x^n + \cdots)}_{= b_m x^m + \cdots}$$

Then:

$\deg g_1(x) < \deg g(x)$

$\Rightarrow$ By hypotheses

$$g_1(x) = q_1(x) f(x) + r_1(x)$$

$$\deg r_1(x) < n = \deg f(x)$$

$$\Rightarrow g(x) = g_1(x) + x^{m-n} a_n^{-1} b_m f(x)$$

$$= (q_1(x) + x^{m-n} a_n^{-1} b_m) f(x) + r_1(x)$$

Take

$$q(x) = q_1(x) + x^{m-n} a_n^{-1} b_m$$

$$r(x) = r_1(x)$$

Uniqueness of $r(x)$

$$g(x) = q(x)f(x) + r(x)$$
$$\|$$
$$\tilde{q}(x)f(x) + \tilde{r}(x)$$

$$\Rightarrow \underbrace{f(x)\left(q(x) - \tilde{q}(x)\right)}_{\deg \geq \deg f(x)} = \underbrace{\tilde{r}(x) - r(x)}_{\deg < \deg f(x)}$$

$$\Rightarrow \boxed{\tilde{r}(x) = r(x)}$$

Rmk: $f(x)$ is monic

$$\Rightarrow \deg\left(f(x)h(x)\right) = \deg f(x) + \deg h(x)$$

Example: The proposition fails for non-monic polynomials

$$f(x) = 2x+1 \in \mathbb{Z}[x]$$
$$g(x) = x$$

Division fails here.

Ideals generated by polynomials

Def^n $f(x) \in \mathbb{R}[x]$

Then the <u>ideal</u> <u>generated</u> <u>by</u> <u>$f(x)$</u>

is the subset

$$(f(x)) = \{a(x)f(x) : a(x) \in \mathbb{R}[x]\}$$

<u>Fact:</u> ① • This is a <u>subgroup</u> <u>of $\mathbb{R}[x]$ under addition</u>

- $a_1(x)f(x) + a_2(x)f(x) = (a_1(x) + a_2(x))f(x)$
- $-a(x)f(x) = (-a(x))f(x)$

We can consider the quotient group $\mathbb{R}[x]/(f(x))$

<u>Fact ②</u> : $\mathbb{R}[x]/(f(x))$ can be equipped with the structure of a commutative ring in a unique way s.t. $\mathbb{R}[x] \longrightarrow \mathbb{R}[x]/(f(x))$

is a homomorphism of rings

Defⁿ If R_1 & R_2 are two commutative rings, a homomorphism of rings or ring homomorphism is a function

$$\varphi : R_1 \longrightarrow R_2$$

s.t. (1) $\forall x, y \in R_1$, $\varphi(x+y) = \varphi(x) + \varphi(y) \in R_2$

(2) $\forall x, y \in R_1$, $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \in R_2$

(3) $\varphi(1_{R_1}) = 1_{R_2} \in R_2$

Pf of Fact 2

$$\pi : R[x] \longrightarrow R[x]/(f(x))$$

Multiplication is well-defined??

$$\pi(h_1(x))\pi(h_2(x)) = \pi(h_1(x)h_2(x))$$

$$\|$$

$$\big(h_1(x) + (f(x))\big) \cdot \big(h_2(x) + (f(x))\big)$$

$$\|$$

$$h_1(x) h_2(x) + (f(x))$$

If we change $h_1(x)$ to

$h_1(x) + q(x) f(x)$

then the product becomes

$$\big(h_1(x) h_2(x) + \underbrace{q(x) f(x) h_2(x)}_{\in (f(x))}\big) + (f(x))$$

$\Rightarrow$ This is equal to

$h_1(x) h_2(x) + (f(x))$.

Define $1 \in R[x]/(f(x))$

$$\|$$

$$1 + (f(x))$$