Ch24: Rings of polynomials

<u>Def</u>: Let A be a commutative ring with unity, and x an arbitrary symbol. Every expression of the form: $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = a(x)$ is called a polynomial in x with coefficients in A, or more simply, a polynomial in x over A. The expressions $a_k x^k$, for $k \in \{1, \cdots, n\}$, are called the terms of the polynomial.

degree of $a(x)$: greatest n s.t. the coefficient of x^n is not zero.

leading coefficient: a_n if degree $a(x) = n$

constant term: a_0

$a(x) = b(x)$: $\deg(a(x)) = \deg(b(x))$ and $a_k = b_k$ for $\forall k \leq \deg(a(x))$

$A[x]$: the set of all the polynomials in x with coefficients in A.

<u>Thm</u>: Let A be a commutative ring with unity. Then $A[x]$ is a commutative ring with unity.

addition: $a(x) = a_0 + a_1x + \cdots + a_nx^n$, $b(x) = b_0 + b_1x + \cdots + b_nx^n$

$$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

multiplication:

$$a(x) \cdot b(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_nx^{2n}$$

$$= \sum_{k=0}^{2n} \left(\sum_{i+j=k} a_ib_j \right) x^k$$

Associativity of multiplication:

$$(a(x) \cdot b(x))\, c(x) = \left(\sum_{k=0}^{2n} \left(\sum_{i+j=k} a_ib_j \right) x^k \right) \left(\sum_{l=0}^{n} c_l x^l \right) = \sum_{m=0}^{3n} \left(\sum_{k+l=m} \left(\sum_{i+j=k} a_ib_j \right) c_l \right) x^m$$

$$a(x)\,(b(x)\,c(x)) = \sum_{m=0}^{3n} \left(\sum_{i+p=m} a_i \left(\sum_{j+l=p} b_jc_l \right) \right) x^m = \sum_{m=0}^{3n} \left(\sum_{(i+j)+l=m}^{\quad ''} a_ib_jc_l \right) x^m$$

Thm: If A is an integral domain, then $A[x]$ is an integral domain.

Pf: Assume $a(x) \neq 0$, $b(x) \neq 0$. $\deg a = m$, $a_m \neq 0$; $\deg b = n$, $b_n \neq 0$. $\xRightarrow{A \text{ is integral domain}} a_m b_n \neq 0$

$\Rightarrow a(x)b(x)$ has a nonzero coefficient: $a_m b_n \Rightarrow a(x)b(x) \neq 0$.

$$\deg[a(x) \cdot b(x)] = \deg a(x) + \deg b(x).$$

From now on assume the coefficient ring is a field denoted by F.

It's NOT true that $F[x]$ is a field. $F[x]$ is only an integral domain

Thm (Division algorithm for polynomials) If $a(x)$ and $b(x)$ are polynomials over a field, and $b(x) \neq 0$, there exist polynomials $q(x)$ and $r(x)$ over F s.t.

$$a(x) = b(x) \cdot q(x) + r(x)$$

and $r(x) = 0$ or $\deg r(x) < \deg b(x)$.

Ex: $F = \mathbb{R}$, $a(x) = x^3 - 2x + 2$, $b(x) = \frac{1}{2}x + 1$

$$\begin{array}{r|l} & 2x^2 - 4x + 4 \\ \hline \frac{1}{2}x + 1 & x^3 + 0x^2 - 2x + 2 \\ & x^3 + 2x^2 \\ \hline & -2x^2 - 2x + 2 \\ & -2x^2 - 4x \\ \hline & 2x + 2 \\ & 2x + 4 \\ \hline & -2 \end{array}$$

$\Rightarrow a(x) = b(x) \cdot (2x^2 - 4x + 4) - 2$

$q(x) = 2x^2 - 4x + 4$, $r(x) = -2$.

Ex: $F = \mathbb{Z}_3$, $a(x) = x^3 - \bar{2}x + \bar{2} = x^3 + x + \bar{2}$, $b(x) = \bar{2}^{-1}x + \bar{1} = \bar{2}x + \bar{1}$

$$
\begin{array}{r|l}
 & \bar{2}x^2+\bar{2}x+\bar{1} \\ \hline
\bar{2}x+\bar{1} & x^3+\bar{0}x^2+x+\bar{2} \\
 & x^3+\bar{2}x^2 \\ \hline
 & \bar{1}x^2+x+\bar{2} \\
 & \bar{4}x^2+\bar{2}x \\ \hline
 & \bar{2}x+\bar{2} \\
 & \bar{2}x+\bar{1} \\ \hline
 & \bar{1}
\end{array}
$$

$\Rightarrow a(x)=b(x)\cdot(\bar{2}x^2+\bar{2}x+\bar{1})+\bar{1}$

$q(x)=\bar{2}x^2+\bar{2}x+\bar{1}$, $r(x)=\bar{1}$

Exer: A.1 $a(x)=2x^2+3x+1$, $b(x)=x^3+5x^2+x$.

$a(x)+b(x)$ in $\mathbb{Z}_5$: $x^3+\bar{7}x^2+\bar{4}x+\bar{1}=x^3+\bar{2}x^2+\bar{4}x+\bar{1}$.

$a(x)\cdot b(x)$ in $\mathbb{Z}_5$: $\bar{2}x^5+(\bar{2}\cdot\bar{5}+\bar{3}\cdot\bar{1})x^4+(\bar{2}\cdot 1+\bar{3}\cdot\bar{5}+\bar{1})x^3+(\bar{3}\cdot\bar{1}+\bar{1}\cdot\bar{5})x^2+(\bar{1}\cdot\bar{1})x$

$=\bar{2}x^5+\overline{13}x^4+\overline{18}x^3+\bar{8}x^2+\bar{1}x$

$=\bar{2}x^5+\bar{3}x^4+\bar{3}x^3+\bar{3}x^2+x$.

A.2 Find the quotient and remainder when x^3+x^2+x+1 is divided by x^2+3x+2 in $\mathbb{Z}[x]$ and in $\mathbb{Z}_5[x]$.

In $\mathbb{Z}[x]$:

$$
\begin{array}{r|l}
 & x-2 \\ \hline
x^2+3x+2 & x^3+x^2+x+1 \\
 & x^3+3x^2+2x \\ \hline
 & -2x^2-x+1 \\
 & -2x^2-6x-4 \\ \hline
 & 5x+5
\end{array}
$$

$q(x)=x-2$, $r(x)=5x+5$

In $\mathbb{Z}_5[x]$:

$$
\begin{array}{r|l}
 & x-2 \\ \hline
x^2+3x+2 & x^3+x^2+x+1 \\
 & x^3+3x^2+2x \\ \hline
 & -2x^2-x+1 \\
 & -2x^2-6x-4 \\ \hline
 & +5x+5=0.
\end{array}
$$

$\Rightarrow q(x)=x-\bar{2}=x+\bar{3}$

$r(x)=\bar{5}x+\bar{5}=\bar{0}$.

A.7. For what values of n is x^2+1 a factor of x^5+5x+6 in $\mathbb{Z}_n[x]$

$$x^5+5x+6 = \underbrace{x^5+x^3}_{x^3(x^2+1)} \underbrace{-x^3-x}_{-x(x^2+1)} + 6x+6 = (x^3-x)(x^2+1)+6x+6$$

x^2+1 is a factor of x^5+5x+6 iff x^2+1 is a factor of $6x+6$ in $\mathbb{Z}_n[x]$

$\Leftrightarrow$ $n=6$ s.t. $6x+6=0$

A.3 Find the quotient and remainder when x^3+2 is divided by $2x^2+3x+4$ in $\mathbb{Q}[x]$, $\mathbb{Z}_3[x]$ and in $\mathbb{Z}_5[x]$.

In $\mathbb{Q}[x]$:

$$\begin{array}{r|l} & \frac{1}{2}x-\frac{3}{4} \\ 2x^2+3x+4 & x^3+0x^2+0x+2 \\ & x^3+\frac{3}{2}x^2+2x \\ \hline & -\frac{3}{2}x-2x+2 \\ & -\frac{3}{2}x-\frac{9}{4}x-3 \\ \hline & \frac{1}{4}x+5 \end{array}$$

$q(x)=\frac{1}{2}x-\frac{3}{4}$, $r(x)=\frac{1}{4}x+5$

In $\mathbb{Z}_3[x]$

$$\begin{array}{r|l} & \bar{2}\cdot x \\ \bar{2}x^2+\bar{3}x+\bar{4} & x^3+0x^2+0\cdot x+\bar{2} \\ & \bar{4}x^3+\bar{6}x^2+\bar{8}x \\ \hline & x+\bar{2} \end{array}$$

$q(x)=\bar{2}x$, $r(x)=x+\bar{2}$

In $\mathbb{Z}_5[x]$

$$\begin{array}{r|l} & \bar{3}x+\bar{3} \\ \bar{2}x^2+\bar{3}x+\bar{4} & x^3+0x^2+0x+\bar{2} \\ & \bar{6}x^3+\bar{9}x^2+\overline{12}x \\ \hline & x^2+\bar{3}x+\bar{2} \\ & \bar{6}x^2+\bar{9}x+\overline{12} \\ \hline & -\bar{6}x+\overline{10}=\bar{4}x \end{array}$$

$q(x)=\bar{3}x+\bar{3}$, $r(x)=\bar{4}x$

A.4 Show that the following is true in $A[x]$ for any ring A: For any odd n

(a) $x+1$ is a factor of x^n+1

(b) $x+1$ is a factor of $x^n+x^{n-1}+\cdots+x+1$

(a): $x^n+1 = x^n+x^{n-1}-x^{n-1}-x^{n-2}+x^{n-2}+x^{n-3}-\cdots-x^2-x+x+1$

$= (x+1)\cdot(x^{n-1}-x^{n-2}+x^{n-3}-\cdots-x+1)$

(b) $x^n+x^{n-1}+\cdots+x+1 = (x+1)(x^{n-1}+x^{n-3}+\cdots+x^2+1)$.

A.5. Prove the following: In $\mathbb{Z}_3[x]$, $x+2$ is a factor of x^m+2, for all m

Prove by induction: · $m=1$: $x+2=x+2$

· Assume $m=k$ holds: $x+2 \mid x^k+2$. Then

$x^{k+1}+\bar{2} = x^{k+1}+\bar{2}\cdot x-\bar{2}\cdot x+\bar{2} = x\cdot(x^k+\bar{2})+(x+\bar{2})$

has $x+\bar{2}$ as a factor. So the statement holds.

Prove: In $\mathbb{Z}_n[x]$, $x+(n-1)$ is a factor of $x^m+(n-1)$ for all m and n.

Pf: $x^m+\overline{(n-1)} = x^m+\overline{(n-1)}\,x+x+\overline{(n-1)} = x\cdot(x^{m-1}+\overline{(n-1)})+x+\overline{(n-1)}$

Prove by induction as before.

A.6 Prove that there is no integer m s.t. $3x^2+4x+m$ is a factor of $6x^4+50$ in $\mathbb{Z}[x]$

Pf: If $6x^4+50=(3x^2+4x+m)\,a(x)$ for $a(x)\in\mathbb{Z}[x]$ then

$6=3a_2$ and $50=m\cdot a_0$, $\deg a=2$

$\Downarrow$

$a_2=2 \Rightarrow a(x)=2x^2+a_1x+a_0$

$(3x^2+4x+m)(2x^2+a_1x+a_0)=6x^4+(3a_1+8)x^3+(3a_0+4a_1+2m)x^2$
$+(4a_0+a_1m)x+a_0m$

$\Rightarrow \begin{cases} 3a_1+8=0 \Rightarrow a_1 \text{ has no solution} \\ \cdots \end{cases}$

$\Rightarrow$ no such $a(x)$.