MODULE V

MORE ALGEBRA – POLYNOMIAL RINGS

To prepare for a study of finite fields (considered in Module VI) we begin with the notion of a ring of polynomials with coefficients from an arbitrary field.

Definition 1. Let F be any field and x be a variable (sometimes called an indeterminant).
Then

$$F[x] = \left\{ \sum_{i=0}^{n} a_i \, x^i \,\middle|\, a_i \in F, \; i = 0, 1, \ldots, n \right\}$$

The elements of $F[x]$ are called polynomials over F (or polynomials with coefficients from F).

If $f(x) = \sum_{i=-}^{n} a_i \, x^i, \; g(x) = \sum_{i=0}^{m} b_i \, x^i$

$$(f + g)(x) = \sum_{i=0}^{\max(n,\, m)} c_i x^i \text{ where } c_i = a_i + b_i$$

$$(f \cdot g)(x) = \sum_{i=0}^{n+m} d_i \, x^i \text{ where } d_i = \sum_{k=0}^{i} a_k \, b_{i-k}.$$

The "0 polynomial" has all coefficients = 0 and we write f = 0. If $f \neq 0$ then deg f = n

where $f(x) = \sum_{i=0}^{n} a_i \, x^i$ and $a_n \neq 0$.

We also define $\deg(0) = -\infty$.

Theorem 1. $(F[x], +, \bullet)$ is a commutative ring with identity.

Some of the Proof: Associativity of + follows easily from associativity of addition in F. Associativity of · is more technical and we leave it as an exercise. Commutativity of both operations follows from commutativity in F. The additive identity is the 0 polynormial and

$$(-f)(x) = \sum_{i=0}^{n} (-a_i) \, x^i \text{ where } f(x) = \sum_{i=0}^{n} a_i \, x^1.$$

The identity of $(F[x], \; \cdot)$ is the polynomial

$$1(x) = 1$$

where 1 is the multplicative identity of F. We leave the distributive law as an exercise.

Observation 1. $\forall$ f, g$\in$ F$[$x$][$deg (f+g) $\leq$ max (deg f, deg g) and deg (f $\cdot$ g) = deg f + deg g$]$
Recall that the ring (Z_n ,$+_n$, $\cdot_n$)has divisors of zeros if n is a compositive number. This is NOT the case for F$[$x$]$.

Observation 2. F$[$x$]$ has NO divisors of 0; hence it is referred to as an integral domain.

Proof If f $\neq$ 0, g$\neq$ 0 then f(x) = $\sum_{k=0}^{n} a_k x^k$, $a_n \neq 0$, and $g(x)=\sum_{i=0}^{m} b_i x^i$, $b_m \neq 0$. Thus

$$(f \cdot g)(x) = a_n b_m x^{n+m} + \sum_{k=0}^{n+m-1} \left(\sum_{i=0}^{k} a_i \, b_{k-i} \right) x^i$$

and, since F is a field, $a_n b_m \neq 0$. Thus f $\cdot$ g$\neq$ 0.

Exercise 1. (Submit this one) Prove that the cancellation law holds, i.e. if $f(x)g(x) = f(x)h(x)$ and f is NOT the zero polynormal then g(x) = h(x).

The reader will recall that in the context of the ring of integers the Division Algorithm played an important role. The same is true here.

Theorem 2. (Division Algorithm) Suppose g(x) and f(x) are polynomials with coefficients from a field F such that deg f $\geq$ 0. Then $\exists$ a unique pair of polynomials, g(x), called the quotient, and r(x), called the remainder, such that g(x) = f(x) q(x) + r(x) and deg r < deg f (Here deg(0) = $-\infty$ and deg(α) = 0 $\forall \alpha \neq 0$, $\alpha \in$ F).

Proof First we prove the existence of q and r.

This proof is analagous to the proof of the Division Algorithm for Z. Consider

$$S = \left\{ g(x) - f(x)\,t(x) \,\middle|\, t(x) \in F[x] \right\}$$

If the zero polynomial belongs to S then $\exists\, q(x) \in F[x]$ such that $g(x) - f(x)\,q(x) = 0$ or, equivalently, $g(x) = f(x)\,q\,(x) + 0$ so $r(x) = 0$ works. Now suppose $0 \notin S$ so that the numbers in

$$D = \left\{ \deg s \,\middle|\, s\,(x) \in S \right\}$$

are non-negative. Choose $r(x) \in S$ such that $\deg r$ is minimum in D. Thus $r(x) = g(x) - f(x)\,q(x)$ for some $q(x) \in F[x]$. We claim that $\deg r < \deg f$. If not consider

$$\hat{r}(x) = r(x) - \alpha\beta^{-1}\ x^{\deg r\, -\, \deg f} f(x)$$

where the leading coefficient of f is β and the leading coefficient of r is α. Since the leading coefficient of the second term in the difference is α and its degree is equal to $\deg r$ it follows that $\deg \hat{r} < \deg r$. But

$$\hat{r}(x) = g(x) - \left(q(x) + \alpha\beta^{-1}\ x^{\deg r\, - \deg f} \right) f(x) \in S$$

is a contradiction. Hence

$$g(x) = f(x)\,q(x) + r(x) \ \text{ and } \ \deg r < \deg f$$

Uniqueness: If $g(x) = f(x)\,q_1(x) + r_1(x) = f(x)\,q_2(x) + r_2(x)$ where $\deg r_1,\ \deg r_2 < \deg f$ then

$$f(x)\left(q_1(x) - q_2(x)\right) = r_2(x) - r_1(x)$$

If $q_i \neq q_2$ then the left side has degree $\geq \deg f$ and the right side has degree $< \deg f$, a contradiction. Hence $q_1 = q_2$ and therefore $r_1 = r_2$ as well.

<u>Definition 2</u>. By the previous theorem $g\,(x) = r\,(x)\ (\text{mod } f(x))$ is unambiguously defined.

Clearly the Division Algorithms and their proofs indicate a strong analogy between the algebraic nature of Z and that of $F[x]$. We continue the development of this analogy by defining "modulo" polynomial arithemtic.

Definition 3. Suppose $\deg f \geq 1$. Then set

$$F[x]/\ (f(x)) = \{r\,(x) \in F[x] |\ \deg\ r < \deg f\}$$ and define

$$r_1(x) \oplus r_2(x) = (r_1(x) + r_2(x))\ (\mathrm{mod}\ f(x))$$

and

$$r_1\ (x) \odot r_2(x) = (r_1(x) \cdot r_2(x))\ (\mathrm{mod}\ f(x))$$

Remark 1. Of course $r_1(x) \oplus r_2(x) = r_1\ (x) + r_2(x)$ since $\deg(r_1 + r_2) < \deg f$. However, $r_1(x) \odot r_2(x)$ is obtained in general by first doing ordinary polynomial multiplication and then employing the Division Algorithm.

Remark 2. Like the integer case a somewhat different approach can be used here and, in some sense, is less mysterious than the one given in Definition 3. Indeed, if we define the equivalence relation $h(x) \equiv g(x)$ if and only if $h(x) - g(x) = 0\ (\mathrm{mod}\ f(x))$ i.e. $h(x) - g(x) = q(x)\ f(x)$ for some $q(x) \in F[x]$ then it follows by the Division Algorithm that the polynomials of degree < deg f constitute a complete collection of distinct representatives of the equivalence classes. Now the definitions:

$$\overline{g(x)} \oplus \overline{h(x)} = \overline{g(x) + h(x)}$$

and

$$\overline{g(x)} \odot \overline{h(x)} = \overline{g(x)\,h(x)},$$

where $\overline{t(x)}$ denotes the equivalence class containing $t(x)$, are unambiguous and reduce to those of Definition 3, if it is decided to always express the equivalence class in terms of its minimum degree element. Moreover this approach greatly reduces the tedium inherent in the proof of our next proposition which we state without proof.

Proposition 1. (c.f. Proposition 1 of Module II) If $f\,(x) \in F[x]$ then $F[x]/\ (f\,(x))$ is a communative ring with identity with respect to the operations $\oplus$ and $\odot$. The additive identity is the zero polynomial and the multplicative identity is given by the constant polynomial 1.

Remark 3. Henceforth we shall drop the use of circles around the addition and multiplication symbols and depend on context to specify which kind of operation is being used, ordinary or modulo f (x).

Recall that Z_n is a field if and only if n is prime. In light of the analogy between $F[x]/\ (f(x))$ and Z_n it is natural to attempt to immitate the notion of a prime number in this context. Recall n is prime provided it doesn't have a NONTRIVIAL factorization i.e. if and only if $\nexists\ 1 < r, s < n$ such that $n = rs$.

Definition 4. The polynomial $f(x) \in F[x]$ is irreducible if and only if $\nexists$ polynomials g, h such that $f = gh$ and $\deg g, \deg h \geq 1$.

Example 1. Consider $x^3 + x \in Z_2[x]$. Then $\left(x^2 + 1\right) x = 0 \pmod{x^3 + x}$ so neither x nor $x^2 + 1$ can possess a multiplicative inverse in $Z_2[x]/\ (x^3 + x)$.

Proof Exercise 2

Our next major task is to establish the fact that $F[x]/\ (f(x))$ is a field if and only if $f(x)$ is irreducible but first we establish more analogies between Z and $F[x]$ leading up to the result. We begin with the notion of an "ideal" in $F[x]$.

Definition 5. The non-empty subset I of $F[x]$ is an ideal if and only

(1) $\forall f(x), g(x) \in I\ (f(x) + g(x) \in I)$

and

(2) $\forall h(x) \in F[x]\ \ \forall f(x) \in I\ (h(x) f(x) \in I)$

Remark 4. We could just as well have used $f(x) - g(x) \in I$ in (1) of the definition.

Proposition 2. If I is an ideal other than $\{0\}$ then $\exists$ a unique MONIC polynomial (leading coefficient = 1) $f(x)$ such that $I = \left(f(x)\right) = \left\{g(x) f(x) \mid g(x) \in F[x]\right\}$

Remark 5. We call $(f(x))$ a principal ideal and because every ideal (even $\{0\}$) in $F[x]$ is principal, $F[x]$ is a principal ideal domain as is the case for Z. Furthermore, we say that I is generated by $f(x)$.

Proof Since $I \neq \{0\}$ there are polynomials in I having non-negative degree. Choose $f(x) \in I$ having minimum non-negative degree and, by virtue of (2) of the definition, assume $f(x)$ to be monic. Now it follows by (2) that $\left(f(x)\right) \subseteq I$. On the other hand, if $h(x) \in I$ then we may write $h(x) = f(x)\, q(x) + r(x)$ where $\deg r < \deg f$ by virtue of the Division Algorithm. But $r(x) = h(x) - f(x)\, q(x) \in I$ so $\deg r = -\infty$, i.e. $r(x)$ is the zero polynomial. Finally then

$$h(x) = f(x)\, q(x) \in (f(x))$$

uniqueness: Exercise 3.

The following discussion leading to the notion of a gcd parallels the integer case.

Proposition 3. If g(x) and h(x) are polynomials in $F[x]$ not both zero then

$$I = \{s(x)\, g(x) + t(x)\, h(x) \mid s(x), t(x) \in F[x]\}$$

is an ideal so that $\exists$ a unique monic polynomial d(x) such that

$$I = (d(x)).$$

The polynomial d(x) is a common divisor of g(x) and h(x) i.e. $\exists$ u(x), v(x) such that g(x) = u(x) d(x) and h(x) = v(x) d(x). Moreover, if $\hat{d}(x)$ is a common divisor of g(x) and h(x) then $\hat{d}(x)$ is a divisor of d(x).

Notation We use $d(x) \mid g(x)$ to denote "d(x) is a divisor of g(x)".

Proof That I is an ideal is trivial to verify. Of course $I \neq \{0\}$ since not both g(x) and h(x) are zero. Thus, by Proposition 1, the existence and uniqueness of d(x) is guaranteed.

If we set s(x) = 1 and t(x) = 0 we see that $g(x) \in I$ so $d(x) \mid g(x)$. Likewise $d(x) \mid h(x)$. Finally, realize that $d(x) \in I$ so that $\exists$ $s_1(x)$, $t_1(x)$ such that $d(x) = s_1(x)\, g(x) + t_1(x)\, h(x)$ and therefore $\hat{d}(x) \mid d(x)$.

Remark 5 and Definition 6. If $g(x), h(x) \in F[x]$ are not both zero then a monic polynomial f(x) is called a greatest common divisor for g(x) and h(x) if $f(x) \mid g(x)$, $f(x) \mid h(x)$ and it has the largest degree of all the common divisors of g(x) and h(x). Obviously the polynomial d(x) of Proposition 3 is such a common divisor as every other common divisor divides d(x). Moreover there is but one greatest common divisor of g(x) and h(x) for if f(x) is a greatest common divisor then the two facts: $f(x) \mid d(x)$ and $\deg f \geq \deg d$, force f = d. Thus gcd (g (x), h(x)) is unambiguous and not only is it the common divisor of largest degree but also every other common divisor divides it.

The reader will also note that gcd (0, 0) is NOT defined as EVERY polynomial divides 0.

Finally, if gcd(g(x), h(x)) = 1 then g(x) and h(x) are relatively prime.

Proposition 4. If f(x) is irreducible and $g(x) \in F[x]$ then $f(x) \mid g(x)$ or gcd(f(x), g(x)) = 1. Also, if $f(x) \mid g(x)\, h(x)$ then $f(x) \mid g(x)$ or $f(x) \mid h(x)$, and this result has an inductive extension, i.e. $f(x) \mid g_1(x) \cdot\cdot g_k(x) \Rightarrow \exists_i$ such that $f(x) \mid g_i(x)$.

Proof Suppose d(x) = gcd (f(x), g(x)) so that $d(x) \mid f(x)$ and $d(x) \mid g(x)$. Then, as f(x) is irreducible either d(x) = 1 or $d(x) = \alpha\, f(x)$ where $\alpha \in F$ and $\alpha \neq 0$. Thus, in the second event, $f(x) = \alpha^{-1} d(x) \mid g(x)$.

Next suppose $f(x) \mid g(x)\, h(x)$. If $f(x)\ \chi\ g(x)$ then by the preceding deduction, $\gcd(f(x), g(x)) = 1$.

But then it follows from Proposition 2 that $\exists s(x), t(x)$ such that $1 = f(x)\, s(x) + g(x)\, t(x)$.

Hence

$$h(x) = f(x)\, s(x)\, h(x) + t(x)\, g(x)\, h(x)$$

and, since $f(x)$ divides both terms of the right hand side, $f(x) \mid h(x)$ as well.

If one scrutinizes the proof of Proposition 3 our next proposition readily follows:

Proposition 5. If $\gcd(f(x), g(x)) = 1$ and $f(x) \mid g(x)\, h(x)$ then $f(x) \mid h(x)$.

Another result with an integer analogy is given next.

Proposition 6 If $\gcd(f(x), g(x)) = 1$, $f(x) \mid h(x)$ and $g(x) \mid h(x)$ then $f(x)\, g(x) \mid h(x)$.

Proof Since $f(x) \mid h(x)$ $\exists\, q(x)$ such that $h(x) = f(x)\, q(x)$.But then, by Proposition 3 and $g(x) \mid f(x)\, q(x)$, it follows that $g(x) \mid q(x)$, i.e. $\exists\, t(x)$ such that $q(x) = g(x)\, t(x)$. Finally then $h(x) = f(x)\, g(x)\, t(x)$ and $f(x)\, g(x) \mid h(x)$.

Proposition 7. If $f_i(x) \mid h(x)$ for $i = 1,\ldots, k$ and $\gcd(f_i(x), f_j(x)) = 1 \forall\, i \neq j$. then $f_1(x)\, f_2(x) \cdots f_k(x) \mid h(x)$.

Proof Exercise 4.

Our next result is in analogy with the very important number theoretic result which we referred to as the Fundamental Theorem of Arithmetic in Module I.

Theorem 3. If $f(x) \in F[x]$ and $\deg f \geq 1$ then $\exists$ unique monic irreducible polynomials $f_1(x),\ldots, f_m(x)$, positive integers $e_1,\ldots, e_m$ and an element $a \in F - \{0\}$ such that

$$f(x) = a\, \left(f_1(x)\right)^{e_1} \left(f_2(x)\right)^{e_2} \cdots \left(f_m(x)\right)^{e_m}.$$

If $\alpha_1, \alpha_2,\ldots, \alpha_k$ are the distinct roots of $f(x) = 0$ in F then $k \leq \deg f$ and k of the irreducible polynomials are of the form $x - \alpha_i$. The others have NO roots in F.

Exercise 5. (Submit this one) Prove this (by induction on deg f).

Just as in the integer case we can characterize the elements of $F[x]\ /(f(x))^*$ using the notion of the gcd.

Theorem 4 $F[x]/(f(x))^* = \{g(x) \in F[x]/f(x))|\ \gcd(g(x), f(x)) = 1\}$

Proof Suppose gcd(g (x), f(x)) = 1 so that by Proposition 2

$\exists$ s(x), t(x) such that g(x) s(x) + f(x) t(x) =1

Thus

$$g(x)\ s(x) = 1 \ (\text{mod } f(x))$$

Now by the Division Algorithm (Theorem2) $\exists$ $h(x) \in F[x]/(f(x))$

such that h(x) = s(x) (mod f(x)) and consequently g(x) h(x) = 1 (mod f(x))

Conversely, if $g(x)^{-1} = h(x)$

then g(x) h(x) = 1 (mod f(x)) i.e. $\exists$ t(x) such that g(x) h(x) + t(x) f(x) = 1.

Thus, if u(x) is a common divisor of g(x) and f(x) it must divide 1 and 1 = gcd (f(x), g(x)).

Corollary 4.1 $F[x]/$ (f(x) is a field if and only if f(x) is irreducible.

Proof If f(x) is irreducible and g(x) $\in$ $F[x]/$ (f(x)) such that $g(x) \neq 0$

then $0 \leq$ deg g < deg f.

Thus f(x) χ g(x) and we may invoke Proposition 4 to conclude that

gcd (f(x)), g(x)) = 1. Hence $F[x]/\ (f(x))^* = F[x]/\ (f(x)) - \{0\}$

Conversely, suppose that f(x) is not irreducible i.e. $\exists$ g(x), h(x) such that f(x) = g(x) h(x) where $1 \leq$ deg g, deg h < deg f. But then g(x), $h(x) \in F[x]/$ (f(x)) and g(x) h(x) = 0 mod (f(x)).

This, of course, implies that g(x) (likewise h(x)) does not have an inverse, else h(x) = 0 -a contradiction. Hence $F[x]/$ (f(x)) is not a field.

Exercise 6. (Submit this one) Consider $F = Z_2$ and $f(x) = x^4 + 1$

Determine $Z_2[x]/\ (x^4 + 1)^*$.

Example 2. Consider $Z_2[x]/\ (x^3 + x + 1)$

Claim $x^3 + x + 1$ is irreducible.

Proof if not $\exists$ a, b, c $\in$ Z_2 such that $x^3 + x + 1 = (x + a)(x^2 + bx + c)$.

But then $a^3 + a + 1 = 0$. However $(0)^3 + (0) + 1 \neq 0$

and $1^3 + 1 + 1 = 1 \neq 0$.

Some of the multiplication table is given below:

	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	x^2	$x+1$	x^2+x+1				
x^2+1	x^2+1	1	x^2				
x^2+x	x^2+x	x^2+x+1	1				
x^2+x+1	x^2+x+1	x^2+1	x				

Exercise 7. (Submit this one)

a) Finish the table

b) With $\alpha = x^2$ compute $\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ and observe that all non-zero elements are generated.

c) Determine all inverses.

Remark We see from b) of the previous exercise that x^2 is a generator of $Z_2\left[x\right]/ \ (x^3+x+1)^*$. Recall from Proposition 2 of Module II that EVERY finite field has a cyclic multiplicative structure.