Mathematics 4300 – Foundations of Algebra – Spring 1999

9. Polynomial Arithmetic. You should think of polynomials as analogues of integers. Like the integers, polynomials have their own arithmetic, and they have a division with remainders. Rational functions are the polynomial version of rational numbers, and all of the material in the last two chapters (especially gcd's and clock arithmetic) have polynomial analogues.

Definition: A **polynomial** in the variable x has the following form:

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_1 x + a_0$$

where the **coefficients** $a_0, a_1, ..., a_d$ are elements of a fixed **field** F.

F can be any of the fields we have encountered so far: $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ or any of the $\mathbf{F}_p$'s coming from clock arithmetic. Let:

$$F[x] = \{\text{polynomials in the variable } x \text{ with coefficients in } F\}$$

Thus we may wish to think about $\mathbf{Q}[x], \mathbf{R}[x], \mathbf{C}[x]$ or one of the $\mathbf{F}_p[x]$.

Examples: Polynomials of low degrees have special names:

(a) **Constant Polynomials** are the polynomials $f(x) = a$ for $a \in F$. We can think of a constant as either a polynomial or as an element of F.

(b) **Linear Polynomials** are of the form $ax + b$, with $a \neq 0$.

(c) **Quadratic polynomials** are of the form $ax^2 + bx + c$, with $a \neq 0$.

Padding Polynomials with Zeroes: We will consider the polynomials:

$$a_d x_d + ... + a_0 \quad \text{and} \quad 0x^{d+1} + a_d x^d + ... + a_0$$

to be the **same**. That is, we can always "pad" a polynomial with zeroes.

That is why we do not consider $0x + b$ to be a linear polynomial. It is really a "padded" constant polynomial, and similarly for $0x^2 + 0x + c$.

Degree: If $f(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_0$ and $a_d \neq 0$, then d is the **degree** of $f(x)$. Thus every polynomial except $f(x) = 0$ has a degree.

(Some people set the degree of 0 to be $-\infty$, but we will leave it undefined).

Examples: (a) The degree of a constant (other than zero) is 0.

(b) The degree of a linear polynomial is 1.

(c) The degree of a quadratic polynomial is 2.

Arithmetic on $F[x]$:

Addition. Addition of polynomials is done coefficient by coefficient:

$$(a_n x^n + ... + a_0) + (b_n x^n + ... + b_0) = (a_n + b_n)x^n + ... + (a_0 + b_0)$$

and if you are given two polynomials which do not start with the same power of x, simply pad the shorter one with zeroes until they do. For example:

$$(ax^2+bx+c)+(dx+e) = (ax^2+bx+c)+(0x^2+dx+e) = ax^2+(b+d)x+(c+e)$$

In fact, $F[x]$ with this addition is a vector space (of infinite dimension!) In any case, just as with finite dimensional vector spaces, properties (a)-(d) of a field are automatic with 0 the additive identity and $-f(x)$ the additive inverse to $f(x)$.

Multiplication. This boils down to $x^d x^e = x^{d+e}$ and "foil". The bookkeeping may be done by multiplying polynomials as you would multiply natural numbers of several digits:

$$\begin{array}{ccccccccc}
 & & a_n x^n & + & \cdots & + & a_1 x & + & a_0 \\
 & \cdot & b_n x^n & + & \cdots & + & b_1 x & + & b_0 \\
\hline
 & & (b_0 a_n) x^n & + & \cdots & + & (b_0 a_1) x & + & b_0 a_0 \\
(b_1 a_n) x^{n+1} & + & (b_1 a_{n-1}) x^n & + & \cdots & + & (b_1 a_0) x & & \\
 & & & & \vdots & & & &
\end{array}$$

For example, in $\mathbf{Q}[x]$, we calculate $(x^2 + 2x + 1)^2$ by:

$$\begin{array}{ccccccccc}
 & & & \cdot & x^2 & + & 2x & + & 1 \\
 & & & & x^2 & + & 2x & + & 1 \\
\hline
 & & & & x^2 & + & 2x & + & 1 \\
 & & 2x^3 & + & 4x^2 & + 2x & & & \\
x^4 & + & 2x^3 & + & x^2 & & & & \\
\hline
x^4 & + & 4x^3 & + & 6x^2 & + & 4x & + & 1
\end{array}$$

It follows from the foil method that:

(e) Multiplication is associative.

(f) Multiplication distributes with addition.

(g) The constant polynomial 1 is the multiplicative identity.

(i) Multiplciation is commutative.

As for (h), we have the following:

Claim: Only the constants (other than 0) have multiplicative inverses.

Proof: If $f(x)$ has degree d and $g(x)$ has degree e, then $f(x)g(x)$ has degree $d+e$. Since the multiplicative identity has degree 0 (it is a constant!) the only way we could have $f(x)g(x) = 1$ would be if $f(x)$ and $g(x)$ were both constants. So $f(x)$ has to be a constant in order to have a multiplicative inverse. Of course, a constant (other than 0) is in the field F, so it always has a multiplicative inverse.

So we don't have reciprocals. But we do have:

Division with Remainders: If $f(x)$ and $g(x)$ are polynomials of degrees d and e, then

$g(x) = f(x)q(x) + r(x)$ where $r(x) = 0$ or else its degree is less than d

Proof: Long division. (This is exactly where we need F to be a field!)

Rational Functions: We define (note the parentheses instead of brackets!)

$$\mathbf{R}(x) = \{\text{“functions” from } \mathbf{R} \text{ to } \mathbf{R} \text{ of the form } \frac{f(x)}{g(x)}\}$$

where $f(x)$ and $g(x)$ are polynomials in $\mathbf{R}[x]$, and $g(x) \neq 0$.

Just as in the case of rational numbers, we have the:

Cross Multiplication Rule: Two fractions are equal as functions:

$$\frac{f(x)}{g(x)} = \frac{f'(x)}{g'(x)}$$

exactly when $f(x)g'(x) = g(x)f'(x)$

The formulas for addition and multiplication should look familiar:

$$\frac{f(x)}{g(x)} + \frac{a(x)}{b(x)} = \frac{f(x)b(x) + a(x)g(x)}{g(x)b(x)}$$

$$\frac{f(x)}{g(x)} \cdot \frac{a(x)}{b(x)} = \frac{f(x)a(x)}{g(x)b(x)}$$

which are well-defined as in our tour of the rational numbers. Armed with these formulas, the arguments from the tour of rational numbers tell us that:

$\mathbf{R}(x)$ **is a field**

Similarly, any $F(x)$ is a field if we **define** two fractions to be the same if they satisfy the cross multiplication rule.

Definitions: (a) $f(x)$ **divides** $g(x)$ if $g(x) = f(x)q(x)$ with zero remainder. In this case we say that $f(x)$ is a **factor** of $g(x)$.

(b) $f(x)$ is **prime** if it has positive degree, and it does not factor as a product of polynomials of smaller degrees. Otherwise it is **reducible**.

Examples: (a) Linear polynomials are always prime(!)

(b) Whether a polynomial is prime or not may depend upon the field. For example:

$$x^2 - 2$$

is prime in $\mathbf{Q}[x]$, but reducible in $\mathbf{R}[x]$ (where it factors as $(x-\sqrt{2})(x+\sqrt{2})$.)

Definition: An element $r \in F$ is a **root** of $f(x)$ if $f(r) = 0 \in F$.

Example: 1 is a root of x^2+1 in $\mathbf{F}_2[x]$ because $1^2+1 = 0$ in $\mathbf{F}_2$. Of course, 1 is not a root of x^2+1 in $\mathbf{Q}[x]$ because $1^2+1 = 2 \neq 0$ in $\mathbf{Q}$.

Observation: r is a root of $f(x)$ if and only if $x - r$ divides $f(x)$.

Proof: Suppose $x-r$ divides $f(x)$. Then $f(x) = (x-r)q(x)$ and $f(r) = 0$. So r is a root of $f(x)$.

On the other hand, suppose r is a root of $f(x)$. Then we may divide $f(x)$ by $x-r$ with remainders to get $f(x) = (x-r)q(x)+a$ where a is a constant! But then $a = 0$ because $f(r) = a$. Thus $x - r$ divides $f(x)$.

Euclid's Algorithm for Polynomials: Starting with polynomials $f(x)$ and $g(x)$ of positive degrees, we repeatedly apply Euclid's algorithm:

$$\begin{array}{rcccc} g(x) & = & f(x)q_1(x) & + & r_1(x) \\ f(x) & = & r_1(x)q_2(x) & + & r_2(x) \\ & & \vdots & & \\ r_{i-1}(x) & = & r_i(x)q_{i+1}(x) & + & r_{i+1}(x) \\ & & \vdots & & \end{array}$$

until we reach a remainder of zero. Let $r_k(x)$ be the last nonzero remainder.

Claim: Euclid's algorithm always terminates.

Proof: Same proof as before! In this case, let d_i be the degree of $r_i(x)$. Then the set:

$$\{d_1, d_2, d_3, ...\}$$

is a decreasing sequence of natural numbers, which must have a smallest element. This smallest element d_k must be the degree of the last nonzero remainder, namely the degree of $r_k(x)$.

Definition: Suppose $f(x)$ and $g(x)$ are nonzero polynomials. Then $d(x)$ is **a greatest common divisor** of $f(x)$ and $g(x)$ if it has the largest degree of any polynomial which divides both $f(x)$ and $g(x)$.

Example: There's a difference between polynomials and natural numbers. Here, greatest common divisors are not unique! For example, in $\mathbf{Q}[x]$:

$$x-1, 2x-2, \text{ and } \frac{1}{2}x - \frac{1}{2} \text{ are all greatest common divisors of}$$

$$x^2-1 \text{ and } x^2-2x+1$$

because they all have the largest possible degree (namely 1), and they all do divide both $x^2-1 = (x-1)(x+1)$ and $x^2-2x+1 = (x-1)^2$.

Proposition 1: The last nonzero remainder in Euclid's algorithm is a greatest common divisor of $f(x)$ and $g(x)$, and any polynomial which divides both $f(x)$ and $g(x)$ also divides any of the gcd's.

Proof: The same proof as before tells us that the last nonzero remainder, which we call $r_k(x)$, is a gcd, and that any common divisor of $f(x)$ and $g(x)$ divides $r_k(x)$. In particular, it also tells us that any gcd divides $r_k(x)$. But if $d(x)$ is a gcd, then it must have the same degree as $r_k(x)$, so that $r_k(x) = d(x) \cdot a$ and $a \in F$. But then $r_k(x)$ divides $d(x)$ as well, since $d(x) = r_k(x) \cdot a^{-1}$, and it follows that any common divisor divides any gcd.

Example: To find a gcd of $x^{10} + 1$ and $x^6 + 1$ in $\mathbf{Q}[x]$:

$$\begin{aligned} x^{10}+1 &= (x^6+1)\cdot(x^4) + (-x^4+1) \\ x^6+1 &= (-x^4+1)\cdot(-x^2) + (x^2+1) \\ -x^4+1 &= (x^2+1)\cdot(-x^2+1) \end{aligned}$$

so the last nonzero remainder, $x^2 + 1$, is a gcd.

Proposition 2: If $d(x)$ is the gcd of $f(x)$ and $g(x)$ coming from Euclid's algorithm, then there are polynomials $a(x)$ and $b(x)$ so that:

$$d(x) = a(x)f(x) + b(x)g(x)$$

Proof: The same as before!

The analogies continue....

Proposition 3: If $p(x)$ is a prime polynomial which divides $f(x)g(x)$, then $p(x)$ divides $f(x)$ or $p(x)$ divides $g(x)$.

Unique Factorization: Every polynomial factors "uniquely" as a product of prime polynomials.

Euclid's Theorem: There are infinitely many prime polynomials.

Remarks: These are all proved as before. There is a slight subtlety in unique factorization. For example:

$$(x-1)(x+1) = (2x-2)(\frac{1}{2}x + \frac{1}{2})$$

but $2x - 2 = 2(x-1)$ and $\frac{1}{2}x + \frac{1}{2} = \frac{1}{2}(x+1)$ and except for this multiplication by "scalars", the terms are unique.

Notice that when the field F is $\mathbf{Q}, \mathbf{R}$ or $\mathbf{C}$, then it is obvious that there are infinitely many prime polynomials since there are already infinitely many linear polynomials! This is much more interesting when the field is $\mathbf{F}_p$, because in that case there are only finitely many linear polynomials but infinitely many prime polynomials by Euclid's theorem. In other words, there are lots of polynomials of larger degrees which are prime.

Clock Arithmetic: Suppose $f(x)$ is a nonzero polynomial. Then we say:

$$a(x) \equiv b(x) \pmod{f(x)}$$

if $a(x)$ and $b(x)$ have the same remainder when divided by $f(x)$.

Equivalence mod $f(x)$ works the same as equivalence mod m

In particular, we have an $f(x)$-clock and more fields:

Proposition 4: If $p(x)$ is prime, then the $p(x)$-clock is a field.

There is also a chinese remainder theorem for polynomials.

An Extended Example: (At last!) Let's start with the field $\mathbf{F}_2$.

As before, we will think of 0 and 1 as being the two elements of $\mathbf{F}_2$, with the funny addition $1+1=0$, and otherwise all additions and multiplications are the ordinary ones.

Prime Polynomials with Coefficients in $\mathbf{F}_2$:

(a) Linear Polynomials: x and $x+1$ are all the linear polynomials. They are both prime because they are linear!

(b) Quadratic Polynomials: x^2, x^2+1, x^2+x and x^2+x+1 are all the quadratic polynomials. The first three are reducible because they obviously factor:

$$x^2 = x \cdot x, x^2 + x = x \cdot (x+1) \text{ and } x^2 + 1 = (x+1)^2$$

(the last one is funny... $2x = 0$ in $\mathbf{F}_2[x]$)

This leaves $f(x) = x^2 + x + 1$. If it were reducible, then it would be a product of two **linear** polynomials, hence it would have a root. But $f(0) = 1$ and $f(1) = 1^2 + 1 + 1 = 1$, so it has no roots. So it is prime.

(c) Cubic Polynomials: Are there any prime ones?

The x^2+x+1-clock (starting with $\mathbf{F}_2[x]$). Recall that we represented the points of a p-clock by their remainders $0,...,p-1$ which are all the numbers between 0 and $p-1$. In the same way, we represent the points of the $p(x)$-clock by their remainders, which are all the polynomials of degree less than the degree of $p(x)$, and the 0 polynomial. In the case of $\mathbf{F}_2[x]$ and the x^2+x+1-clock, the possible remainders are therefore:

$$0, 1, x, x+1$$

so this clock has exactly 4 elements. In other words, we've found a field with 4 elements! Hooray! Let's work out the addition and multiplication tables:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

So there you have it, your very own field with 4 elements!

Some food for thought:

(1) We've found fields with $2, 3, 4, 5$ elements. There is no field with 6 elements! There are fields with $7, 8, 9$ elements but none with 10 elements. Yes for 11 and 13, but none for $12, 14$ and 15. Yes for 16 and 17, but none for 18. What is the pattern?

(2) Let $p(x) = x^2 + 1$. This is prime when the field is $\mathbf{R}$. Moreover, I claim that the $p(x)$-clock in this case is the field of complex numbers!!

Exercises:

1. Divide $x^7 + 1$ by $x^3 + x^2 + x + 1$ with remainders:

(a) In the polynomial ring $\mathbf{Q}[x]$.

(b) In the polynomial ring $\mathbf{F}_2[x]$.

(c) In the polynomial ring $\mathbf{F}_3[x]$.

2. Find a gcd of the two polynomials above in each of the three cases.

3. Find a field with 8 elements. That is:

(a) Find a prime cubic (i.e. degree 3) polynomial $p(x) \in \mathbf{F}_2[x]$.

(b) Construct the $p(x)$-clock and write out the multiplication table.

4. Find a field with 9 elements.

5. List all the prime quadratic polynomials in $\mathbf{F}_5[x]$.

6. (a) Find a prime cubic polynomial of degree 3 in $\mathbf{Q}[x]$.

(b) Prove that every cubic polynomial in $\mathbf{R}[x]$ is reducible.

(c) Find a prime quadratic polynomial in $\mathbf{R}[x]$.

(d) Prove that every quadratic polynomial in $\mathbf{C}[x]$ is reducible.