April 2, 2009

Recall that we constructed our sets of numbers as **N→Z→Q→R→C**

N is a (commutative) **semigroup**, which is a set of numbers that are commutative and associative, meaning that we have a set **N** and an operation (+) so that the following is true for any a, b, c € **N:** a + b € **N** (closure); a + b = b + a (commutativity); and a + (b + c) = (a + b) + c (associativity). Note that N is both an additive semigroup and a multiplicative one.

A **monoid** is a set *M* with binary operation *: *M* x *M* → *M,* with the following axioms:

- associativity : for all a, b, c in *M*, (a*b)*c = a*(b*c)
- identity element: there exists an element e in *M*, such that for all a in *M,* a*e =e*a = a
- closure: for all a, b in *M*, a*b is in *M*.

That is, it is a semigroup with an identity. **N** is a multiplicative monoid (the identity is 1). The whole numbers (**N** ∪ {0}) form a commutative monoid (with + as the operation).

Z, is an additive **group** , which is a monoid with the additional property of inverses, i.e. for all a in a set *S*, there exists a^{-1} so that $a^{-1}*a = a*a^{-1} = e$. Note that it is not possible to make **Z** into a multiplicative group. However, **Z** is a **ring:** it is an additive group and a multiplicative monoid, together with distributive laws for combining the two operations.

Q forms a **field**, which is a ring in which every nonzero member has a multiplicative inverse. For example, **R** and **C** are fields, but **Z** is not (since ½ is not an element of **Z**).

Now we turn to polynomials in, which we form by extending a field by an element x.

By a field extension, we let K be an arbitrary field, and use K[x] to be any finite sum of a product of an element of K with a nonnegative power of x. We have seen such field extensions before; for example we saw that the complex numbers can be thought of as

R[i] = { a + bi | a, b real numbers}. Here we only need the first power, since i^2=-1. Another example we mentioned was **Q**[$\sqrt[3]{2}$] = { a + b $\sqrt[3]{2}$ + c $\sqrt[3]{4}$ | a, b, c rational}. Again, we only need consider $\sqrt[3]{2}$ and $\sqrt[3]{4}$ because $(\sqrt[3]{2})^3$=2, which is rational.

Coming back to our polynomials, each polynomial has the form:

$$a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x + a_0$$

with each coefficient a_i being an element of K.

K[x] is a ring, like **Z**.

Let's compare these two rings - **Z** and **K**[x].

INTEGERS **Z**	POLYNOMIALS **K**[x]
Addition and Subtraction Example: 7-8 = -1	Addition and Subtraction Example: $(3x+5) - (x^2) = -x^2 + 3x + 5$
Multiplication Example: 2*8 = 16	Multiplication Example: $(3x + 5)(2x^2 + 1) = 6x^3 + 10x^2 + 3x + 5$
Not always Division Example: 6/2 = 3, but 7/2 is NOT in **Z**	Not always Division Example: $(x^2 - 1)(x + 1) = x - 1$, $(x^2 - 1)/2x$ is not in **Q**[x]
Factor Example: 18 = 3*3*2	Factor Example: $(x^2 - 1) = (x + 1)(x - 1)$
Primes Example: Irreducible integers 2, 3, 5, 7	Primes Example: Irreducible Polynomials 2x+4

Factoring

Z: To factor an integer x means we can write x as r*s, where r and s are both less than x. Therefore prime numbers can't be factored, since the only divisors of p are 1 and p; that is, p = 1*p by definition and p isn't less than itself.

K[x]: To factor a polynomial f(x) means we can write f(x) as h(x) * g(x), where the degree of h(x) is less than f(x) and the degree of g(x) is less than f(x). Therefore a polynomial, 2x+4 can't be

reduced, since 2x+4 = 2(x+2) and the degree of 2 is 0 and the degree of x+2 is 1, which is not less than the degree of 2x+4, which is also 1.

The **Euclidean Algorithm** is a method in determining the greatest common factor of 2 numbers, a and b, using the following steps:

$b = aq_1 + r_1$

$a = r_1q_2 + r_2$

$r_1 = r_2q_3 + r_3$

$r_2 = r_3q_4 + r_4$

.

.

.

$r_{n-2} = r_{n-1}q_n + r_n$

$r_{n-1} = r_nq_{n+1} + 0$

where r_i represents remainders and q_i represents the quotients.

The last non-zero remainder, r_n is the greatest common factor of a and b, or as we write gcd(b,a) = d.

Since $b = aq_1 + r_1$, then by definition of divisibility the greatest common factor of a and b, d , divides $b - aq_1$, and $r_1 = b - aq_1$. Therefore,

$$\gcd(b,a) = \gcd(a,r_1) = \gcd(r_1, r_2) = \ldots. = \gcd(r_{n-2}, r_{n-1}) = r_n.$$

As an example, we can find the gcd of 1071 and 1029.

Note that $1071 = 1029 \times 1 + 42$.

Now $1029 = 42 \times 24 + 21$,

and $42 = 21 \times 2 + 0$.

This tells us that gcd(1071,1029) = 21.

We can use this method to find the greatest common factor of polynomials as well.

Find gcf ($x^5 – 17x + 2$, $x^2 – 4x + 4$).

The answer should be x-2, let's use long division with polynomials and the Euclidean Algorithm to verify this.

$(x^5 – 17x + 2) = p(x) * (x^2 – 4x + 4) + r(x)$

What are p(x) and r(x)? We can use long division of polynomials to find out. Remember, this works just like long division of numbers, we just have to pay a little more attention.

$$
\begin{array}{rl}
 & x^3 + 4x^2 + 12x + 32 \\
x^2 – 4x + 4 \;) & x^5 \qquad\qquad\qquad – 17x + 2 \\
 & \underline{x^5 – 4x^4 + 4x^3} \\
 & \quad 4x^4 - 4x^3 \\
 & \quad \underline{4x^4 - 16x^3 + 16x^2} \\
 & \qquad 12x^3 - 16x^2 - 17x \\
 & \qquad \underline{12x^3 - 48x^2 + 48x} \\
 & \qquad\quad 32x^2 - 65x + 2 \\
 & \qquad\quad \underline{32x^2 - 128x - 128} \\
 & \qquad\qquad\quad 63x - 126
\end{array}
$$

So, we have determined that

$$x^5 – 17x + 2 = (x^2 – 4x + 4)(x^3 + 4x^2 + 12x + 32) + (63x - 126)$$

For the next step, we need to calculate gcd($x^2 – 4x + 4$, $63x - 126$)

But since $63x-126 = 63(x-2)$, we see that $x^2 – 4x + 4 = (63x-126)(x-2)/63 + 0$

Thus, the greatest common factor of $x^5 – 17x + 2$ and $x^2 – 4x + 4$ is x-2, as we expected.

While the Euclidean algorithm seems to be more work than it is worth here (since we can just factor each part and look for common terms), note that will still works when factoring is not so easy (or even not possible).

For example, suppose we want the common factor of $x^4 - 4x^3 + 4x^2 - 3x + 14$ and $x^4 + 8x^3 + 12x^2 + 17x + 6$.

Dividing gives us

$$x^4 + 8x^3 + 12x^2 + 17x + 6 = (x^4 - 4x^3 + 4x^2 - 3x + 14)*1 + (12x^3 + 8x^2 + 20x - 8)$$

We can rewrite the remainder as $12(x^3 + 2x^2/3 + 5x/3 - 2/3)$ to make the division a little easier (constant multiples don't matter), so we have

$$x^4 + 8x^3 + 12x^2 + 17x + 6 = (x^3 + 2x^2/3 + 5x/3 - 2/3)(x + 22/3) + (x^2 + x + 2)*(49/9)$$

and finally we have

$$12x^3 + 8x^2 + 20x - 8 = (x^2 + x + 2)(12x - 4) + 0$$

Thus, the greatest common factor is $x^2 + x + 2$, despite the fact that I didn't realize that $x^2 + x + 2$ was a factor of either polynomial when we started.