Appendix A PhL 6.20.13

This has been installed.

Appendix A. Tale of Two Rings 1
1. Multiplication Example 1
2. Division Example 1 3
3. Division Example 2 7

Appendix A. Tale of Two Rings

Here we ask the question: Is there some kind of analogy between real numbers and polynomials when the real numbers are written in usual decimal notation and when the polynomials have coefficients which lie in Mod(10) so they can also be written in a decimal notation. We pursue this question first in terms of multiplication and then later division.

1. Multiplication Example

Define an ∞-tuple of Mod(10) elements as something having this form

.....xxxxxxx.xxxxxx.....

For particular ∞-tuples, we need only show the required digits, as for example for 2242.457. That is, we ignore the infinite set of leading zeros and the infinite set of trailing zeros.

(a) We can represent a base-10 number (like 2242.457) as an ∞-tuple of elements each of which lie in field Z_{10} = Mod(10). Such ∞-tuples themselves form a ring which has a 1-to-1 correspondence with the ring of real numbers. Let's call this ring R_1. We have a certain familiar rule for the multiplication of such ∞-tuples in R_1. The rule is that we convert each ∞-tuple to a real number, get the product of the two real numbers, and then convert the result back to an ∞-tuple. This rule is very effectively implemented by a calculator. For example

22.16 * 3.42 = 75.7872

Since the real numbers form a field, R_1 is also a field, but we are mostly concerned with its ring sense.

(b) On the other hand, we can represent a polynomial f(z) having coefficients in Mod(10) as a an ∞-tuple of elements each in Z_{10} = Mod(10). For example,

22.16 = the ∞-tuple for polynomial f(z) = $2z^1 + 2z^0 + 1z^{-1} + 6z^{-2}$

The "decimal point" is placed just before any negative powers which might be present.

Such ∞-tuples form a ring we shall call R_2. We have a rule for multiplying these ∞-tuples; it is just "what we do" when we multiply polynomials whose coefficients lie in Mod(10). The result can also be represented as an ∞-tuple. For example (notice for example that $12z^{-4}$ is replaced by $2z^{-4}$)

$$(2z + 2 + 1z^{-1} + 6z^{-2}) \bullet (3 + 4z^{-1} + 2z^{-2}) = (6z + 4 + 5z^{-1} + 6z^{-2} + 6z^{-3} + 2z^{-4}) .$$

It is easy to have Maple multiply polynomials in this manner, so we can then verify the above hand calculation:

```
f1 := 2*z + 2 + 1/z + 6/z^2:
f2 := 3 + 4/z + 2/z^2:
f := expand(f1*f2) mod 10;
```

$$f := 6z + 4 + 5\frac{1}{z} + 6\frac{1}{z^2} + 6\frac{1}{z^3} + 2\frac{1}{z^4}$$

The upshot is that, in ring R_2 we have

$$22.16 \bullet 3.42 = 64.5662$$

The ∞-tuple product here is not the real number 64.5622, it is the ∞-tuple which represents the polynomial shown above in R_2.

The point so far is that the product of two ∞-tuples depends on which ring these ∞-tuples belong to.

In Section 3 (a) of Ref [Galois] this ring R_2 is simply called R, and it is shown that it really is a ring and has a multiplicative identity. This ring can be defined just for "proper" polynomials (non-negative powers only), or for general polynomials (all powers allowed).

(c) The real number multiplication shown in (1) above can be done as follows:

```
 22.16
  3.42
   .4432
  8.864
 66.48
 75.7872
```

In this process, carries are maintained both in computing partial product rows and then in adding up those rows.

(d) The polynomial multiplication shown in (2) above can be done as follows:

```
 22.16
  3.42
   .4422
  8.844
```

```
  66.38
  64.5662
```

In this process, carries are discarded both in computing partial product rows and then in adding up those rows. This is the way Mod(10) math works.

2. Division Example 1

(a) We continue to represent a base-10 number (like 2242.457) as an ∞-tuple of elements each of which lie in field Z_{10} = Mod(10). As noted above, such ∞-tuples themselves form a ring R_1 which has a 1-to-1 correspondence with the ring of real numbers. We have a certain familiar rule for the *division* of such ∞-tuples in R_1. The rule is that you convert each ∞-tuple to a real number, get the quotient of the two real numbers, and then convert the result back to an ∞-tuple. This rule is very effectively implemented by a calculator (such as Maple). For example,

22.16 / 3.42 = 6.479532164.....

Since this example is a rational number, the decimals go into a repeating pattern. For 70 digits,

```
Digits := 70:
22.16/3.42;
      6.4795321637426900584795321637426900584795321637426900584795321637426900
```

and one sees that

6.479532163742690058 479532163742690058 479532163742690058 479532163742690...

(b) On the other hand, we can represent a polynomial f(z) as a an ∞-tuple of elements each in Z_{10} = Mod(10). For example

22.16 = the ∞-tuple for polynomial f(z) = $2z^1 + 2z^0 + 1z^{-1} + 6z^{-2}$

Such ∞-tuples form a ring R_2. We have a rule for dividing these ∞-tuples; it is what we do when we do long division of polynomials whose coefficients lie in Mod(10). The result can also be represented as an ∞-tuple.

For example

$(2z + 2 + 1z^{-1} + 6z^{-2}) / (3 + 4z^{-1} + 2z^{-2}) = 4z + 2 + 5z^{-1} + 4z^{-2} + 8z^{-3} + 0z^{-4} + 8z^{-5} + ...$

22.16/3.42 = 42.54808....

(c) To find the ratio of two ∞-tuples in R_1, we can do long division by the usual method. For example,

```
          6.479.....
342  |  2216.0000
```

```
2054        6
 1640
 1368       4
  2720
  2394      7
   3260
   3078     9
                 .......
```

Each time the divisor is multiplied by a quotient integer, there is *carry*. And each time there is a subtraction to obtain a new current dividend, there is *borrow*.

(d) To carry out a polynomial division in R_2, one method is to carry out the long division algorithm, armed with a multiplication and addition table for Mod(10). For example, things start off this way:

```
          42.54808 .........
342 |  2216.0000
       268            4
        636
        684           2
         520
         500          5
          200
          268         4
           420
           426        8
            40
            00        0
            400
            426       8
                          .......
```

At each stage of the process, there is *no carry* when the divisor is multiplier by a quotient integer, and there is *no borrow* when the subtraction is done at each stage to get the new current divisor.

Our conclusion about carries and borrows for division is thus very similar to that for multiplication found earlier.

The above manual method for polynomial division in R_2 is quite tedious but could of course be automated. For illustration, here is another method which allows a simple Maple evaluation of the quotient coefficients.

We know that the division O(z) = I(z)/H(z) (with all positive and negative powers allowed) results in the following time-domain equation for the polynomial coefficients,

$$i_n = \sum_{j=-\infty}^{\infty} h_j \, o_{n+j} \quad . \qquad (1.9.5)$$

Multiplying top and bottom by z^2, our division example above becomes (we redefine I and H),

$$(2z^3 + 2z^2 + 1z + 6) / (3z^2 + 4z + 2) = I(z) / H(z)$$

giving us a proper polynomial for H(z). In our ∞-tuple notation, this says

22.16/3.42 = 2216/342 .

This last line is true *not* because we multiply top and bottom by 100, because the ratio does not refer to the division of real numbers. It is true because of the way polynomial division is defined:

$$n(z)/d(z) = q(z) \Leftrightarrow n(z) = q(z)d(z) \Leftrightarrow [z^s n(z)] = q(z)\,[z^s\, d(z)] \Leftrightarrow [z^s n(z)]/\,[z^s\, d(z)] = q(z) \; .$$

In general, we can therefore always slide the "decimal point" in numerator and denominator by the same number of positions in either direction, just as we can when dividing ∞-tuples in the real field R_1.

As a counterexample, suppose we were to multiply our division ratio above top and bottom by 5. We would get (everything is Mod(10)) :

$$(2z^3 + 2z^2 + 1z + 6) / (3z^2 + 4z + 2) = (10z^3 + 10z^2 + 5z + 30) / (15z^2 + 20z + 10)$$

$$= (5z) / (5z^2) = z^{-1} \qquad \text{// not true !}$$

Now, given our new H(z) shown above, the time-domain equation simplifies to,

$$i_n = \sum_{j=0}^{2} h_j \, o_{n+j} = h_0 o_n + h_1 o_{n+1} + h_2 o_{n+2} \quad . \qquad (1.9.5)$$

This can be regarded as the following recursion relation,

$$h_2 o_{n+2} = i_n - h_0 o_n - h_1 o_{n+1}$$

or

$$o_{n+2} = (i_n/h_2) - (h_0/h_2) o_n - (h_1/h_2) o_{n+1}$$

or

$$o_{n+2} = a\, i_n - b o_n - c o_{n+1} \qquad a \equiv (1/h_2) \qquad b \equiv (h_0/h_2) \qquad c \equiv (h_1/h_2)$$

in our example: $a \equiv (1/3) = 7$ $b \equiv (2/3) = 4$ $c \equiv (4/3) = 8$

The integer results for a,b,c are those of Mod(10). For example

a = 3^{-1} = 7, since 3*7 = 21 = 1
b = 2*3^{-1} = 2*7 = 14 = 4
c = 4*3^{-1} = 4*7 = 28 = 8 .

Using our usual manner of denoting the coefficients of I(z) and O(z) we have

I(z) = $i_{-3}\,z^3 + i_{-2}z^2 + i_{-1}z + i_0$ // in our example = $2z^3 + 2z^2 + 1z + 6$

O(z) = $o_{-1}z + o_0 + o_1z^{-1} + o_2z^{-2} + o_3z^{-3} + \ldots$..

We know that the leading coefficient of O(z) is o_{-1} as shown just looking at our polynomial ratio. All o_j prior to this vanish.

Here then is Maple code to compute the o_j coefficients for $(2z^3 + 2z^2 + 1z + 6) / (3z^2 + 4z + 2)$:

```
for j from -10 to 100 do i[j] := 0 od:          # clear out all i values
i[-3] := 2: i[-2] := 2: i[-1] := 1: i[0] := 6:  # set non-zero i values
a := 7: b := 4: c := 8:                         # set parameters
o(-3) := 0: o(-2) := 0:                         # initial values
for n from -3 to 40 do    # use recursion relation to compute the o values
     o(n+2) := a*i[n] - b*o(n) - c*o(n+1) mod 10;
od:
x := seq(o(n),n=-1..40);  # display these values
```

$$x := 4, 2, 5, 4, 8, 0, 8, 6, 0, 6, 2, 0, 2, 4, 0, 4, 8, 0, 8, 6, 0, 6, 2, 0, 2, 4, 0, 4, 8, 0, 8, 6, 0, 6, 2, 0, 2, 4, 0, 4, 8, 0$$

The first 20 terms of the quotient polynomial O(z) are then

```
unprotect(O): O := 0:   # it happens that O is the Order-Of function in Maple
for n from -1 to 20 do  # construct the polynomial O(z) from the o(n)
  O := O + o(n)*z^(-n);
  od:
O;
```

$$4z+2+5\frac{1}{z}+4\frac{1}{z^2}+8\frac{1}{z^3}+8\frac{1}{z^5}+6\frac{1}{z^6}+6\frac{1}{z^8}+2\frac{1}{z^9}+2\frac{1}{z^{11}}+4\frac{1}{z^{12}}+4\frac{1}{z^{14}}+8\frac{1}{z^{15}}+8\frac{1}{z^{17}}+6\frac{1}{z^{18}}+6\frac{1}{z^{20}}$$

We can verify our truncated O(z) result by multiplying it times H(z) to see how close we come to I(z):

```
H := 3*z^2+4*z+2:
I_ := 2*z^3+2*z^2+1*z+6:
expand(O*H - I_) mod 10: sort(%);
```

$$4\frac{1}{z^{19}}+2\frac{1}{z^{20}}$$

We have now shown that our example polynomial division has this result,

$(2z + 2 + 1z^{-1} + 6z^{-2}) / (3 + 4z^{-1} + 2z^{-2}) = 4z + 2 + 5z^{-1} + 4z^{-2} + 8z^{-3} + 0z^{-4} + \ldots..$

We can write this in terms of R_2 ring ∞-tuples in this manner

221.6 / 34.2 = 42.5480....

The ∞-tuple product here is not the real number 42.5488...., it is the ∞-tuple which represents the polynomial shown above in R_2.

From the Maple output we in fact have

22.16 / 3.42 = 42.5 480860620240 480860620240 480860620240 480 ....

and we see that the sequence 480860620240 repeats forever.

We conclude then by comparing the R_1 and R_2 ∞-tuple division notations:

R_1 22.16 / 3.42 = 6.479532163742690058 479532163742690058 479532163742690058 ....

R_2 22.16 / 3.42 = 42.5 480860620240 480860620240 480860620240 ....

3. Division Example 2

What happens now if we shuffle a pair of coefficients in the previous division example? Suppose we have this polynomial division of interest, where the 4 and 3 have been swapped,

$(2z + 2 + 1z^{-1} + 6z^{-2}) / (4 + 3z^{-1} + 2z^{-2}) = ???$

As before multiply top and bottom by z^2 to get

$(2z^3 + 2z^2 + 1z + 6) / (4z^2 + 3z + 2) \equiv I(z) / H(z)$.

In the ∞-tuple world of the real number ring R_1 we can write

22.16/4.32 = 2216/432 = 5.1 296 296 296 .....

with no complications. But something new appears in our R_2 ring polynomial division. The numerator is unchanged, and the output sequence o_j still begins with o_{-1} . The recursion relation is the same but with these new parameters

$o_{n+2} = a\, i_n - b o_n - c o_{n+1}$ $a \equiv (1/h_2)$ $b \equiv (h_0/h_2)$ $c \equiv (h_1/h_2)$

in our example: $a \equiv (1/4)$ $b \equiv (2/4)$ $c \equiv (3/4)$

Maple can do the polynomial division in terms of real polynomial coefficients,

```
for j from -10 to 100 do i[j] := 0 od:          # clear out all i values
i[-3] := 2: i[-2] := 2: i[-1] := 1: i[0] := 6:  # set non-zero i values
a := (1/4): b := (2/4): c := (3/4):             # set parameters
o(-3) := 0: o(-2) := 0:                         # initial values
for n from -3 to 40 do    #use recursion relation to compute the o values
     o(n+2) := a*i[n] - b*o(n) - c*o(n+1);
od:
x := seq(o(n),n=-1..8);  # display these values
```

$$x := \frac{1}{2}, \frac{1}{8}, \frac{-3}{32}, \frac{193}{128}, \frac{-555}{512}, \frac{121}{2048}, \frac{4077}{8192}, \frac{-13199}{32768}, \frac{6981}{131072}, \frac{84649}{524288}$$

```
unprotect(O): O := 0:   # it happens that O is the Order-Of function in Maple
for n from -1 to 8 do  # compute the polynomial O(z) = I(z)/H(z)
  O := O + o(n)*z^(-n);
  od:
O;
```

$$\frac{1}{2}z + \frac{1}{8} - \frac{3}{32}\frac{1}{z} + \frac{193}{128}\frac{1}{z^2} - \frac{555}{512}\frac{1}{z^3} + \frac{121}{2048}\frac{1}{z^4} + \frac{4077}{8192}\frac{1}{z^5} - \frac{13199}{32768}\frac{1}{z^6} + \frac{6981}{131072}\frac{1}{z^7} + \frac{84649}{524288}\frac{1}{z^8}$$

```
H := 4*z^2+3*z+2:
I_ := 2*z^3+2*z^2+1*z+6:
expand(O*H - I_): sort(%);
```

$$\frac{309795}{524288}\frac{1}{z^7} + \frac{84649}{262144}\frac{1}{z^8}$$

where in the last line we again verify the truncated quotient so obtained.

The *problem* is that in our R_2 ∞-tuple ring world we need a quotient polynomial which has coefficients in the ring Mod(10). It is easy to show that, for general Mod(2n), no even element has an inverse. For example, 4 does not have an inverse in Mod(10) since

4*0 = 0
4*1 = 4
4*2 = 8
4*3 = 12 = 2
4*4 = 16 = 6
4*5 = 20 = 0
4*6 = 24 = 4
4*7 = 28 = 8
4*8 = 32 = 2
4*9 = 36 = 6

Notice that 1 is missing from the list. One reason it is missing is that all the numbers in the right column must be even!

Therefore, there is no way to write our quotient,

$(2z^3 + 2z^2 + 1z + 6) / (4z^2 + 3z + 2) = (1/2)z + (1/8) - (3/32)z^{-1} + ...$

such that the quotient has coefficients in Mod(10). This says that in the ring R_2 the quotient of the two polynomials does not exist. Thus we end up with the following conclusions for Example 2

R_1 22.16 / 3.42 = 2216 / 342 = 6.479532163742690058 479532163742690058 ....

R_2 22.16 / 3.42 = 2216 / 342 = does not exist

If instead of Mod(10) we were to use symbols from Mod(p) where p is a prime number, then all elements have inverses and this problem cannot arise. An example would be Mod(7) with digits 0,1,2,3,4,5,6. Of course in this case, the ratios for R_1 would be written in base-7 math.