UNIVERSITY OF WYOMING
Math 4520—Fall 2024
Algebra III
Fields
Department of Mathematics

Polynomials, Power Series and Such

1. Power Series

Let S be the ring consisting of all infinite sequences $a = (a_0, a_1, a_2, \ldots)$ of real numbers $a_i \in \mathbb{R}$ with componentwise addition

$$(a_0,\, a_1,\, a_2,\, \ldots) + (b_0,\, b_1,\, b_2,\, \ldots) = (a_0{+}b_0,\, a_1{+}b_1,\, a_2{+}b_2,\, \ldots)$$

and multiplication defined by

$$(a_0,\, a_1,\, a_2,\, \ldots)(b_0,\, b_1,\, b_2,\, \ldots) = (a_0b_0,\, a_0b_1{+}a_1b_0,\, a_0b_2{+}a_1b_1{+}a_2b_0,\, \ldots).$$

A straightforward but tedious check shows that S satisfies all the required axioms and so is a bona fide ring. A more insightful approach is to show that S is isomorphic to the set $\mathbb{R}[\![t]\!]$ consisting of all power series in t with real coefficients: elements of $\mathbb{R}[\![t]\!]$ are expressions of the form

$$a(t) = a_0 + a_1t + a_2t^2 + \cdots \qquad \text{where } a_0, a_1, a_2, \ldots \in \mathbb{R}.$$

To formalize this argument, we consider the obvious bijection $\theta : S \to \mathbb{R}[\![t]\!]$ given by $(a_0, a_1, a_2, \ldots) \mapsto a_0 + a_1t + a_2t^2 + \cdots$; then for any two sequences $a = (a_0, a_1, a_2, \ldots)$ and $b = (b_0, b_1, b_2, \ldots)$ in S, we have

$$\begin{aligned}\theta(a+b) &= \theta\big((a_0{+}b_0,\, a_1{+}b_1,\, a_2{+}b_2,\, \ldots)\big) = (a_0{+}b_0) + (a_1{+}b_1)t + (a_2{+}b_2)t^2 + \cdots\\ &= (a_0{+}a_1t{+}a_2t^2 + \cdots) + (b_0{+}b_1t{+}b_2t^2 + \cdots) = \theta(a) + \theta(b)\end{aligned}$$

and

$$\begin{aligned}\theta(ab) &= \theta\big((a_0b_0,\, a_0b_1{+}a_1b_0,\, a_0b_2{+}a_1b_1{+}a_2b_0,\, \ldots)\big)\\ &= a_0b_0 + (a_0b_1{+}a_1b_0)t + (a_0b_2{+}a_1b_1{+}a_2b_0)t^2 + \cdots\\ &= (a_0{+}a_1t{+}a_2t^2 + \cdots)(b_0{+}b_1t{+}b_2t^2 + \cdots) = \theta(a)\theta(b).\end{aligned}$$

Thus θ is an isomorphism: $S \cong \mathbb{R}[\![t]\!]$.

If Calc II is still fresh in your mind, with all of its warnings about checking for domain of convergence of infinite series, then feel free to ignore all of that. We are *not* doing calculus here, simply because we are not considering functions. While it is true in the context of a calculus course that power series are useful for the representation of certain functions, *we are not concerned at all with functions here!* So for the time being, you are better off ignoring anything you might remember about convergence. As an example, from the calculus viewpoint the two series

$$\begin{aligned} f_1(t) &= \sum_{k=0}^{\infty} k!t^k = 1+t+2t^2+6t^3+24t^3+\cdots \\ \text{and}\quad f_2(t) &= \sum_{k=0}^{\infty} k!^2t^k = 1+t+4t^2+36t^3+576t^3+\cdots \end{aligned}$$

converge only at $t=0$ (their radius of convergence is zero) so they represent the same function, and a very trivial function at that. From our viewpoint, t is not a number, but rather just a symbol to help us remember how to add and multiply power series; $f_1(t)$ and $f_2(t)$ are just two (very different) elements of $\mathbb{R}[[t]]$ which should be treated just like two (different) sequences $(1,1,2,6,24,\ldots)$, $(1,1,4,36,576,\ldots)$ in S. All of this should be viewed as liberating, and not at all burdensome; rather it is the calculus student who, because of the role of series (for representing functions $\mathbb{R}\to\mathbb{R}$) must carry the extra burden of having to worry about convergence. For us this burden is nonexistent.

We refer to $\mathbb{R}[[t]]$ as the *ring of power series in t with real coefficients*. Some textbooks instead refer to $\mathbb{R}[[t]]$ as the ring of *formal* power series in t with real coefficients; however, the word 'formal' here is redundant since every power series is by definition a formal construct.

Now we may freely replace the coefficient ring $\mathbb{R}$ by any other commutative ring with identity, such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{F}_p$, etc. to obtain new rings of power series denoted by $\mathbb{Z}[[t]]$, $\mathbb{Q}[[t]]$, $\mathbb{F}_p[[t]]$, etc. For example in $\mathbb{F}_2[[t]]$ we have

$$(1+t^2+t^5+t^6+t^7+\cdots)(1+t+t^3+t^4+t^7+\cdots) = 1+t+t^2+t^4+t^6+t^7+\cdots.$$

Here it should be observed that products in $\mathbb{F}_2[[t]]$ are quite well-defined, and they *do not* represent functions $\mathbb{F}_2\to\mathbb{F}_2$ (after all, infinite sums of elements of $\mathbb{F}_2$ are completely meaningless).

The ring $\mathbb{R}[[t]]$ is clearly a commutative ring with identity 1 (corresponding to the sequence $(1,0,0,0,\ldots)\in S$ in the old description). What are the units of S? Suppose that $\mathbb{R}[[t]]$ contains series

$$u(t) = u_0+u_1t+u_2t^2+\cdots \quad\text{and}\quad v(t) = v_0+v_1t+v_2t^2+\cdots$$

such that $u(t)v(t)=1$; equivalently,

$$\begin{aligned} u_0v_0 &= 1; \\ u_0v_1+u_1v_0 &= 0; \\ u_0v_2+u_1v_1+u_2v_0 &= 0; \end{aligned}$$

etc. This has a solution for v iff $u_0 \neq 0$; for then we solve to obtain

$$\begin{aligned} v_0 &= u_0^{-1};\\ v_1 &= -u_0^{-2}u_1;\\ v_2 &= u_0^{-3}u_1^2 - u_0^{-1}u_2; \end{aligned}$$

etc. So a series $u(t) \in \mathbb{R}[\![t]\!]$ has an inverse iff its constant term is nonzero. In the same way, an element $u(t) \in \mathbb{Z}[\![t]\!]$ is a unit iff its constant term is ± 1 (a unit in $\mathbb{Z}$). More generally we have

Theorem 1. If R is any commutative ring with identity, then $R[\![t]\!]^\times = R^\times$; i.e. every unit in the ring $R[\![t]\!]$ has only one term (a constant term).

For example, consider $u(t) = 1 + t - t^3 \in \mathbb{Q}[\![t]\!]$ which is a unit since its constant term is a nonzero rational number. In order to determine $v(t) = u(t)^{-1} \in \mathbb{Q}[\![t]\!]$, we solve

$$(1 + t - t^3)(v_0 + v_1t + v_2t^2 + v_3t^3 + v_4t^4 + v_5t^5 + \cdots) = 1$$

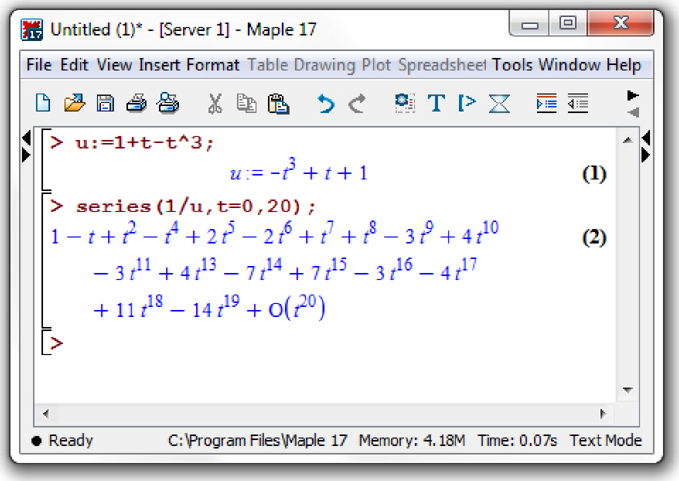
for the coefficients in $v(t) = v_0 + v_1t + v_2t^2 + \cdots$. This gives

$$\left.\begin{aligned} v_0 &= 1\\ v_0 + v_1 &= 0\\ v_1 + v_2 &= 0\\ v_0 + v_1 - v_3 &= 0\\ v_1 + v_2 - v_4 &= 0\\ v_2 + v_3 - v_5 &= 0\\ \text{etc.}& \end{aligned}\right\} \quad \Rightarrow \quad \left\{\begin{aligned} v_0 &= 1\\ v_1 &= -1\\ v_2 &= 1\\ v_3 &= 2\\ v_4 &= 0\\ v_5 &= 3\\ \text{etc.}& \end{aligned}\right.$$

and so

$$v(t) = \frac{1}{u(t)} = \frac{1}{1+t-t^3} = 1 - t + t^2 + 2t^3 + 3t^5 + \cdots .$$

Observe the recurrence formula $v_n = v_{n-2} + v_{n-3}$ for all $n \geq 3$. This approach does not give an explicit closed formula for v_n, but at least we can find as many terms in $v(t)$ as needed. (A closed formula for v_n is possible, but to explain this would be too much of a digression from our current focus.) Using MAPLE®, we may compute the first any desired terms in the series expansion of $v(t)$ as follows:


Untitled (1)* - [Server 1] - Maple 17
File Edit View Insert Format Table Drawing Plot Spreadsheet Tools Window Help
Ready
C:\Program Files\Maple 17 Memory: 4.18M Time: 0.07s Text Mode

```
> u:=1+t-t^3;
                    u := -t^3 + t + 1                         (1)
> series(1/u,t=0,20);
1 - t + t^2 - t^4 + 2 t^5 - 2 t^6 + t^7 + t^8 - 3 t^9 + 4 t^10    (2)
    - 3 t^11 + 4 t^13 - 7 t^14 + 7 t^15 - 3 t^16 - 4 t^17
    + 11 t^18 - 14 t^19 + O(t^20)
>
```

Here we have generated only the first 20 terms; but an obvious modification in the command will generate many more terms, hundreds if desired.

2. Polynomials

A polynomial may be regarded as a power series with only finitely many nonzero coefficients. Thus, for example, the polynomial

$$4 - 3t + 7t^2 + 5t^4$$

corresponds to the sequence $(4, -3, 7, 0, 5, 0, 0, 0, \dots) \in S$ under the previous description. Denote by $\mathbb{R}[t]$ the ring of all polynomials in t with real coefficients, i.e. the set of all expressions of the form

$$a_0 + a_1t + a_2t^2 + \cdots + a_nt^n$$

where $a_0, a_1, \dots, a_n \in \mathbb{R}$. We say that a_k is the *coefficient* of t^k, for $k = 0, 1, 2, \dots, n$. In the same way, $\mathbb{Z}[t]$, $\mathbb{Q}[t]$ and $\mathbb{F}_p[t]$ denote the sets of polynomials in x with coefficients in $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{F}_p$ respectively; more generally, if R is any commutative ring with identity, then $R[t]$ denotes the ring of polynomials in t with coefficients in R. The *zero polynomial,* denoted by 0, is the polynomial whose coefficients are all zero. Two polynomials $f(t)$ and $g(t)$ are the *same,* denoted $f(t) = g(t)$, if their corresponding coefficients are the same; for example,

$$1 - 2t + 5t^3 = 5t^3 - 2t + 1 = 1 - 2t + 0t^2 + 5t^3 = 0t^4 + 5t^3 + 0t^2 - 2t + 1$$

since in each of these polynomials corresponds to the same sequence of coefficients $(1, -2, 0, 5, 0, 0, 0, \dots) \in S$. In particular, we write $f(t) = 0$ if and only if all coefficients of $f(t)$ are zero; thus for example, $t^2 - 1 \neq 0$. If $p(t) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n \neq 0$, the *degree* of $p(t)$, denoted by $\deg p(t)$, is the largest k such that $a_k \neq 0$. For example, $\deg(1-2t+5t^3)=3$, $\deg(2t-0t^2)=1$, $\deg(-8)=0$. We define $\deg 0 = -\infty$ so that the following proposition holds universally for all polynomials $f(t), g(t)$, with the obvious conventions for adding $-\infty$.

Proposition 2. If $f(t), g(t) \in \mathbb{R}[t]$ then $\deg\big(f(t)g(t)\big) = \deg f(t) + \deg g(t)$. The same result holds in $R[t]$ where R is any integral domain.

Proof. If either of the two polynomials $f(t), g(t)$ is zero, then $f(t)g(t)=0$ and the desired equality holds, with both sides equal to $-\infty$ by convention. We may therefore assume $f(t)$ and $g(t)$ are nonzero polynomials. Now

$$f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n; \quad g(t) = b_0 + b_1 t + b_2 t^2 + \cdots + b_m t^m$$

where $n = \deg f(t)$ and $m = \deg g(t)$; in particular, $a_n \neq 0$ and $b_m \neq 0$. Thus

$$f(t)g(t) = a_0 b_0 + (a_0 b_1 + a_1 b_0)t + \cdots + a_n b_m t^{n+m}$$

where the last term is the unique term of highest degree in $f(t)g(t)$, with coefficient $a_n b_m \neq 0$; thus

$$\deg\big(f(t)g(t)\big) = n + m = \deg f(t) + \deg g(t).$$

□

We say that $f(t)$ *divides* $g(t)$ in $\mathbb{R}[t]$, denoted $f(t) \,\big|\, g(t)$, if $g(t) = m(t)f(t)$ for some $m(t) \in \mathbb{R}[t]$. The following is obviously analogous to the Division Algorithm for Integers. We omit the proof, which we take to be evident from the usual algorithm of long division.

Theorem 3 (Division Algorithm for Polynomials). Let F be a field and suppose $f(t), d(t) \in F[t]$ such that $d(t) \neq 0$. Then there exist unique polynomials $q(t), r(t) \in F[t]$ such that

$$f(t) = q(t)d(t) + r(t), \qquad \deg r(t) < \deg d(t)\,.$$

As usual 'unique' means that there is only one pair of polynomials $(q(t), r(t))$ satisfying the conclusions of the theorem. We call $q(t)$ and $r(t)$ the quotient and remainder, respectively. Note that $d(t) \,\big|\, f(t)$ if and only if $r(t) = 0$. The Division Algorithm holds for $F[t]$ whenever F is a field, but not for $R[t]$ with a more general coefficient ring R; in particular the Division Algorithm does not hold in $\mathbb{Z}[t]$.

A *zero* or *root* of a polynomial $f(t)$ is a number a such that $f(a) = 0$. An important consequence of the Division Algorithm is the fact (made explicit by the following theorem) that roots of polynomials correspond to linear factors.

Theorem 4. Let $f(t) \in F[t]$ and $a \in F$ where F is a field. Then $f(a) = 0$ if and only if $(t-a) \mid f(t)$.

Proof. If $(t-a) \mid f(t)$ then $f(t) = (t-a)m(t)$ for some $m(t) \in F[t]$, and so $f(a) = 0m(a) = 0$.

Conversely, suppose $f(a) = 0$. By the Division Algorithm, we may write $f(t) = (t-a)q(t) + r(t)$ for some $q(t), r(t) \in F[t]$ where $r(t)$ has degree less than 1 (the degree of $t-a$). If $r(t) = 0$ then we would have $(t-a) \mid f(t)$, and so we would be done. So let's assume instead that $r(t) \neq 0$, in which case $\deg r(t) = 0$, so $r = r(t)$ is a nonzero constant. Substituting a for t gives $0 = f(a) = 0m(a) + r$, so $r = 0$. This contradiction proves that in fact $(t-a) \mid f(t)$. □

This argument extends to multiple roots:

Theorem 5. Let F be a field. If $f(t) \in F[t]$ has distinct roots $a_1, a_2, \ldots, a_n \in F$, then $f(t)$ is divisible by $(t-a_1)(t-a_2)\cdots(t-a_n)$. In particular, either $f(t) \neq 0$ or $\deg f(t) \geq n$.

Proof. Suppose $f(t)$ has at least n distinct roots $a_1, a_2, \ldots, a_n$. By Theorem 3, we have $f(t) = (t-a_1)g(t)$ for some $g(t) \in F[t]$. Substituting a_2 for t gives $0 = f(a_2) = (a_2 - a_1)g(a_2)$ where $a_2 - a_1 \neq 0$ since the n roots are distinct. Therefore $g(a_2) = 0$, and by Theorem 3 we have $g(t) = (t-a_2)h(t)$ for some $h(t) \in F[t]$. Thus $f(t) = (t-a_1)(t-a_2)h(t)$. Continuing in this way, we eventually obtain $f(t) = (t-a_1)(t-a_2)(t-a_3)\cdots(t-a_n)m(t)$ for some $m(t) \in F[t]$. □

Corollary 6. Let F be a field. A nonzero polynomial $f(t) \in F[t]$ of degree n cannot have more than n distinct roots. □

It is possible to state this result more generally in $R[t]$ where R is an integral domain; but the result does not hold if the coefficient ring contains zero divisors. For example, the nonzero polynomial $x^2-1 \in \mathbb{Z}_{24}$ has roots $1, 5, 7, 11, 13, 17, 19, 23 \in \mathbb{Z}_{24}$, i.e. all units of $\mathbb{Z}_{24}$. Here there are eight distinct roots in $\mathbb{Z}_{24}$, far more than the degree of the polynomial x^2-1.

Let F be a field. Given two polynomials $f(t), d(t) \in F[t]$, we say that $d(t)$ *divides* $f(t)$ if $f(t) = q(t)d(t)$ for some $q(t) \in F[t]$. In this case we write $d(t) \bigm| f(t)$ and we also say that $d(t)$ is a *divisor of* $f(t)$, or that $f(t)$ *is a multiple of* $d(t)$. If $d(t)$ divides $f(t)$, then $cd(t)$ also divides $f(t)$ whenever $c \in F^\times$; so we might as well choose c so that the leading coefficient in $d(t)$ (i.e. the coefficient in the highest degree term) is 1. Such a polynomial is called *monic*. Given two nonzero polynomials $f(t), g(t) \in F[t]$, list the monic polynomials dividing $f(t)$ (this will be a finite list, even if F is infinite, since we only consider monic divisors) and all monic polynomials dividing $g(t)$. There is at least one polynomial in both lists (the constant polynomial 1). There is exactly one polynomial of highest degree in both lists, called the *greatest common divisor* of $f(t)$ and $g(t)$, denoted $\gcd(f(t), g(t))$. This is most readily computed by Euclid's Algorithm.

Theorem 7 (The Extended Euclidean Algorithm for Polynomials). Let F be any field, and let $f(t)$ and $g(t)$ be nonzero polynomials in $F[t]$. Then there exist polynomials $u(t), v(t) \in F[t]$ such that

$$u(t)f(t) + v(t)g(t) = \gcd(f(t), g(t)).$$

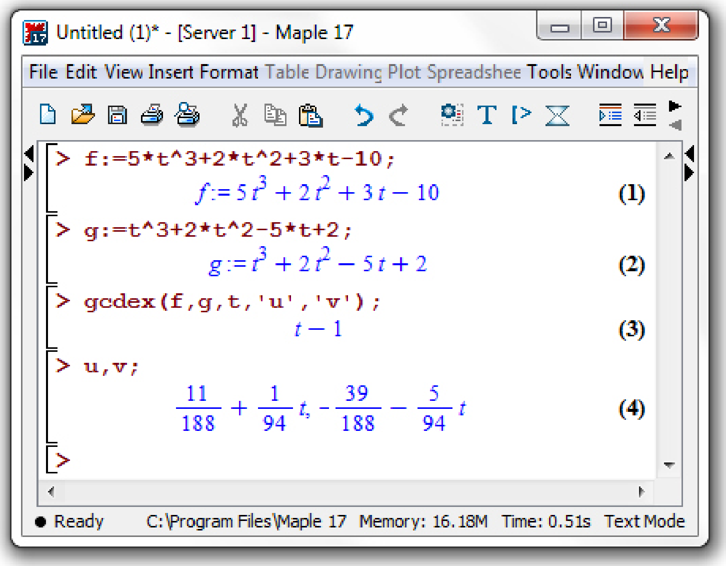
Example: Compute the gcd of the polynomials $f(t) = 5t^3 + 2t^2 + 3t - 10$, $g(t) = t^3 + 2t^2 - 5t + 2 \in \mathbb{Q}[t]$. The steps are almost the same as when computing the gcd of two integers, but with a twist:

$$\begin{aligned}
f(t) &= 5g(t) + (-8t^2 + 28t - 20)\\
g(t) &= \big(-\tfrac{1}{8}t - \tfrac{11}{16}\big)(-8t^2 + 28t - 20) + \big(\tfrac{47}{4}t - \tfrac{47}{4}\big)\\
-8t^2 + 28t - 20 &= \tfrac{4}{47}\big(-8t + 20\big)\big(\tfrac{47}{4}t - \tfrac{47}{4}\big) + 0
\end{aligned}$$

At this point we might want to say that $\gcd(f(t), g(t)) = \frac{47}{4}t - \frac{47}{4} = \frac{47}{4}(t-1)$. However observe that the much simpler polynomial $t-1$ divides both $f(t)$ and $g(t)$. In order to have a unique answer when computing gcd's, we will insist that the gcd be a **monic** polynomial, i.e. that its leading coefficient be 1. Thus in this case $\gcd(f(t), g(t)) = t - 1$ and the extended form of the algorithm allows us to write this as a polynomial-linear combination of $f(t)$ and $g(t)$:

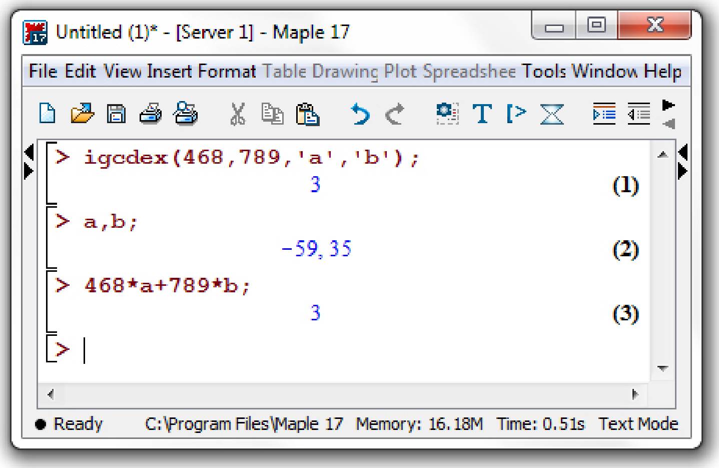
$$\begin{aligned}
\tfrac{47}{4}t - \tfrac{47}{4} &= g(t) - \big(-\tfrac{1}{8}t - \tfrac{11}{16}\big)(-8t^2 + 28t - 20);\\
t - 1 &= \tfrac{4}{47}g(t) + \big(\tfrac{1}{94}t + \tfrac{11}{188}\big)(-8t^2 + 28t - 20)\\
&= \tfrac{4}{47}g(t) + \big(\tfrac{1}{94}t + \tfrac{11}{188}\big)\big(f(t) - 5g(t)\big)\\
&= \big(\tfrac{1}{94}t + \tfrac{11}{188}\big)f(t) + \big(-\tfrac{5}{94}t - \tfrac{39}{188}\big)g(t).
\end{aligned}$$

Here is a MAPLE® session that computes $\gcd(f(t), g(t))$, *and* finds polynomials $u(t), v(t)$ such that $u(t)f(t) + v(t)g(t) = \gcd(f(t), g(t))$:


Untitled (1)* - [Server 1] - Maple 17
File Edit View Insert Format Table Drawing Plot Spreadsheet Tools Window Help
● Ready C:\Program Files\Maple 17 Memory: 16.18M Time: 0.51s Text Mode

```
> f:=5*t^3+2*t^2+3*t-10;
                f := 5 t^3 + 2 t^2 + 3 t - 10                (1)
> g:=t^3+2*t^2-5*t+2;
                 g := t^3 + 2 t^2 - 5 t + 2                  (2)
> gcdex(f,g,t,'u','v');
                           t - 1                             (3)
> u,v;
             11     1       39     5
            ---- + ---- t, - ---- - ---- t                    (4)
            188     94      188    94
>
```

Note that the command `gcdex` performs the Extended Euclidean Algorithm on polynomials; the corresponding command for integers is `igcdex`.


Untitled (1)* - [Server 1] - Maple 17
File Edit View Insert Format Table Drawing Plot Spreadsheet Tools Window Help
● Ready C:\Program Files\Maple 17 Memory: 16.18M Time: 0.51s Text Mode

```
> igcdex(468,789,'a','b');
                           3                                 (1)
> a,b;
                        -59, 35                              (2)
> 468*a+789*b;
                           3                                 (3)
> |
```

A polynomial $f(t) \in R[t]$ of degree ≥ 1 is *reducible* if $f(t) = a(t)b(t)$ where the polynomials $a(t), b(t) \in R[t]$ both have degree ≥ 1. If $f(t)$ does not factor in this way, then $f(t)$ is *irreducible*. This is not new terminology; here we have just specialized it to the context of polynomial rings.

Theorem 8 (Euclid's Lemma for polynomials). Let F be a field, and suppose that an irreducible polynomial $p(t)$ divides $a(t)b(t)$ where $a(t), b(t) \in F[t]$. Then either $p(t) \mid a(t)$ or $p(t) \mid b(t)$.

Proof. Suppose $p(t) \not| \, a(t)$; then $\gcd(p(t), b(t) = 1$ so there exists $u(t), v(t) \in F[t]$ such that $u(t)p(t) + v(t)a(t) = 1$. Then $p(t)$ divides $u(t)p(t)b(t) + v(t)a(t)b(t) = b(t)$ since $p(t)$ divides both of the terms on the left hand side. □

The same argument used in the proof of the Fundamental Theorem of Arithmetic gives the same result for polynomial rings of the form $F[t]$ where F is any field:

Theorem 9 (Unique Factorization for $F[t]$). Let F be a field, and suppose the polynomial $f(t) \in F[t]$ has degree ≥ 1. Then there exists a constant $c \in F^\times$ and monic irreducible polynomials $p_1(t), p_2(t), \ldots, p_k(t) \in F[t]$ such that

$$f(t) = cp_1(t)p_2(t) \cdots p_k(t).$$

This factorization is unique up to permutation of the irreducible factors.

Note that c is the leading coefficient of $f(t)$; and the problem of 'migration of units' is taken care of by simply factoring out a scalar factor c from the right hand side so that all irreducible factors can be assumed to be monic.

Examples: In $\mathbb{F}_2[t]$, both polynomials of degree 2 (namely t and $1 + t$) are irreducible. There are four polynomials of degree 2, namely t^2, $1 + t^2 = (1 + t)^2$, $t + t^2 = t(1 + t)$ and $1 + t + t^2$. Of these, three have roots in $\mathbb{F}_2$, and the other one is irreducible since it has no roots (check that neither 0 nor 1 is a root of $1 + t + t^2$, so $1 + t + t^2$ has no linear factor, hence is irreducible).

In $\mathbb{F}_3[t]$, the three monic polynomials of degree 1 (namely t, $1 + t$ and $2 + t$) are irreducible. There are nine monic polynomials of degree 2. Six of these are reducible:

$$\begin{aligned} &t^2; \\ t(1+t) &= t + t^2; \\ t(2+t) &= 2t + t^2; \\ (1+t)(1+t) &= 1 + 2t + t^2; \\ (1+t)(2+t) &= 2 + t^2; \\ (2+t)(2+t) &= 1 + t + t^2. \end{aligned}$$

So the remaining three monic polynomials of degree 2 (namely $1 + t^2$, $2 + t + t^2$ and $2 + 2t + t^2$) are irreducible. Similarly, there are eight monic irreducible polynomials of degree three:

$$\begin{array}{cccc} 1 + 2t^2 + t^3, & 1 + t + 2t^2 + t^3, & 1 + 2t + t^3, & 1 + 2t + t^2 + t^3, \\ 2 + t^2 + t^3, & 2 + t + t^2 + t^3, & 2 + 2t + t^3, & 2 + 2t + 2t^2 + t^3. \end{array}$$

To check that each of these polynomials of degree 3 is irreducible, it suffices to check that none of the elements $0, 1, 2 \in \mathbb{F}_3$ is a root. If you only want to count *how many* monic irreducible polynomials of degree 3 there are, note that there are 27 monic polynomials of degree 3, then subtract 10 (the number of monic polynomials with 3 linear factors), and also subtract 9 (the number of polynomials having two monic irreducible factors, one of degree 1 and one of degree 2).

Counting irreducible polynomials of degree 4 is more delicate. For example, the polynomial $t^4 + 1 \in \mathbb{F}_3[t]$ has no roots in $\mathbb{F}_3 = \{0, 1, 2\}$, but it is reducible since it factors as $1 + t^2 + t^4 = (1 + t + t^2)(1 + 2t + t^2)$. In order to check that a polynomial of degree 4 is irreducible, you may first check that it has no roots (hence no factor of degree 1), and then check that it is not divisible by any of the irreducible polynomials of degree 2 (which hopefully you have previously found).

3. Rational Expressions (Rational Functions)

Let F be any field. Denote by $F(t)$ the set of all quotients of the form $\frac{f(t)}{g(t)}$ where $f(t), g(t) \in F[t]$ and $g(t) \neq 0$. It is not hard to see that $F(t)$ is in fact a field. Elements of $F(t)$ are called *rational expressions in t with coefficients in F*. It is also common to refer to elements of $F(t)$ as *rational functions in t*; but this leads to a problem: if we expect $\frac{t^3+t^2+1}{t^2+t} \in \mathbb{F}_2(t)$ to represent a function, what is its domain and range? It certainly does not represent a function $\mathbb{F}_2 \to \mathbb{F}_2$ since its denominator vanishes at every element of $\mathbb{F}_2 = \{0, 1\}$. For now, the best advice is to (once again) treat t as merely a symbol, and to perform all operations of addition, subtraction, multiplication and division in $F(t)$ symbolically.

Note that the field $F(t)$ contains $F[t]$ as a subring; this just says that every polynomial may be regarded as a rational function (with constant denominator 1). In fact $F(t)$ is constructed from $F[t]$ in the same way that $\mathbb{Q}$ is constructed from $\mathbb{Z}$. This process works more generally if we start with any *integral domain* R (i.e. R is a commutative ring with identity, having no zero divisors): the set of all symbols $\frac{a}{b}$ (for $a, b \in R$ with $b \neq 0$) forms a field, called the *quotient field of R*, containing R as a subring. So $\mathbb{Q}$ is the quotient field of the ring $\mathbb{Z}$; and in the same way, for any field F, the field $F(t)$ of rational functions in t is the quotient field of the polynomial ring $F[t]$.

4. Laurent Series

Again, let F be a field. A *Laurent series in t with coefficients in F* is an expression of the form

$$f(t) = \sum_{n=k}^{\infty} a_n t_n = a_k t^k + a_{k+1} t^{k+1} + a_{k+2} t^{k+2} + a_{k+3} t^{k+3} + \cdots$$

where $k \in \mathbb{Z}$ and $a_k, a_{k+1}, a_{k+2}, a_{k+3}, \ldots \in F$. Note that k (the index of the first term) is allowed to be a negative integer. Note that every power series is a Laurent series (in which we take $k = 0$). We denote by $F(\!(t)\!)$ the set of all Laurent series in t with coefficients in F. Then $F(\!(t)\!)$ is a ring which, by the previous remark, contains $F[\![t]\!]$ as a subring. In fact, $(\!(t)\!)$ is the quotient field of $F[\![t]\!]$. Moreover, $F(\!(t)\!)$ has a subring isomorphic to $F(x)$, in the same way that $F[\![t]\!]$ has a subring isomorphic to $F[t]$. These containments are illustrated in the diagram

$$\begin{tikzcd}
& \{\text{Laurent series}\} = F(\!(t)\!) \arrow[dl, dash] \arrow[dr, dash] & \\
\{\text{rational functions}\} = F(t) \arrow[dr, dash] & & F[\![t]\!] = \{\text{power series}\} \arrow[dl, dash] \\
& F[t] = \{\text{polynomials}\} &
\end{tikzcd}$$

How exactly does one recognize $F(x)$ as a subring of $F(\!(t)\!)$? In other words, how does one rewrite every rational function as a Laurent series? One approach uses the geometric series

$$\frac{1}{1-u} = 1 + u + u^2 + u^3 + u^4 + u^5 + \cdots .$$

So for example given a rational function

$$r(t) = \frac{1+2t+7t^2}{2t-5t^2+9t^3} \ \in \ \mathbb{Q}(t),$$

With a little bit of rewriting, we have

$$\begin{aligned}
r(t) &= \frac{1+2t+7t^2}{2t} \cdot \frac{1}{1-\left(\frac{5}{2}t - \frac{9}{2}t^2\right)} \\
&= \left(\tfrac{1}{2}t^{-1} + 1 + \tfrac{7}{2}t\right)\left[1 + \left(\tfrac{5}{2}t - \tfrac{9}{2}t^2\right) + \left(\tfrac{5}{2}t - \tfrac{9}{2}t^2\right)^2 + \left(\tfrac{5}{2}t - \tfrac{9}{2}t^2\right)^3 + \cdots\right] \\
&= \left(\tfrac{1}{2}t^{-1}+1+\tfrac{7}{2}t\right)\left[1 + \left(\tfrac{5}{2}t-\tfrac{9}{2}t^2\right) + \left(\tfrac{25}{4}t^2-\tfrac{45}{2}t^3+\tfrac{81}{4}t^4\right) + \left(\tfrac{125}{8}t^3-\tfrac{675}{8}t^4+\tfrac{1215}{8}t^5-\tfrac{729}{8}t^6\right) + \cdots\right] \\
&= \left(\tfrac{1}{2}t^{-1} + 1 + \tfrac{7}{2}t\right)\left[1 + \tfrac{5}{2}t + \tfrac{7}{4}t^2 - \tfrac{55}{8}t^3 + \cdots\right] \\
&= \tfrac{1}{2}t^{-1} + \tfrac{9}{4} + \tfrac{55}{8}t + \tfrac{113}{16}t^2 + \cdots \ \in \ \mathbb{Q}(\!(t)\!).
\end{aligned}$$

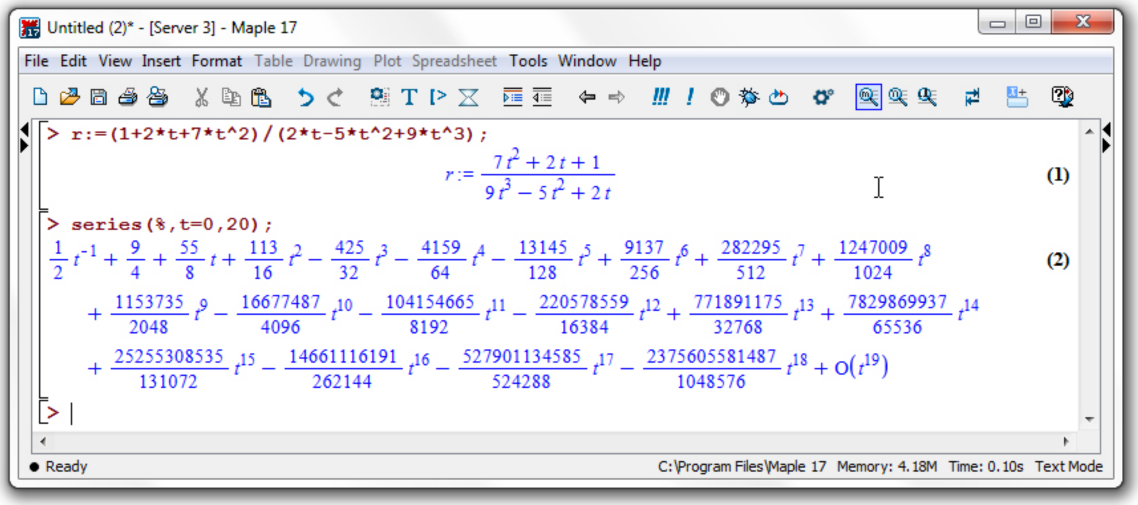
Clearly this approach requires some care with the arithmetic details; nevertheless you can see from this example how, at least in principle, any rational function can be expanded as a Laurent series. An alternative, possibly more practical, approach is to write

$$1 + 2t - 7t^2 \ = \ \left(2t - 5t^2 + 9t^3\right)r(t)$$

so the first term in $r(t)$ must be $\frac{1}{2}t^{-1}$. Now we write $r(t) = \frac{1}{2}t^{-1} + r_0 + r_1 t + r_2 t^2 + \cdots$ and so

$$1 + 2t - 7t^2 \ = \ \left(2t - 5t^2 + 9t^3\right)\left(\tfrac{1}{2}t^{-1} + r_0 + r_1 t + r_2 t^2 + \cdots\right).$$

This yields a sequence of linear equations allowing us to solve for $r_0 = \frac{9}{4}$, $r_1 = \frac{55}{8}$, $r_2 = \frac{113}{16}$, etc. Let's check using MAPLE®:



Untitled (2)* - [Server 3] - Maple 17
File Edit View Insert Format Table Drawing Plot Spreadsheet Tools Window Help

```
> r:=(1+2*t+7*t^2)/(2*t-5*t^2+9*t^3);
```

$$r := \frac{7t^2+2t+1}{9t^3-5t^2+2t} \qquad (1)$$

```
> series(%,t=0,20);
```

$$\frac{1}{2}t^{-1}+\frac{9}{4}+\frac{55}{8}t+\frac{113}{16}t^2-\frac{425}{32}t^3-\frac{4159}{64}t^4-\frac{13145}{128}t^5+\frac{9137}{256}t^6+\frac{282295}{512}t^7+\frac{1247009}{1024}t^8 \qquad (2)$$
$$+\frac{1153735}{2048}t^9-\frac{16677487}{4096}t^{10}-\frac{104154665}{8192}t^{11}-\frac{220578559}{16384}t^{12}+\frac{771891175}{32768}t^{13}+\frac{7829869937}{65536}t^{14}$$
$$+\frac{25255308535}{131072}t^{15}-\frac{14661116191}{262144}t^{16}-\frac{527901134585}{524288}t^{17}-\frac{2375605581487}{1048576}t^{18}+\mathrm{O}(t^{19})$$

```
> |
```

● Ready   C:\Program Files\Maple 17 Memory: 4.18M Time: 0.10s Text Mode

Working over a finite coefficient field such as $\mathbb{F}_p$ is actually much easier than working over $\mathbb{Q}$, because saves us from having to manipulate ugly fractions as in the previous example. Suppose for example we want to expand the rational function

$$h(t) = \frac{2+t+t^3}{t^3+2t^5+2t^7} \in \mathbb{F}_3(t)$$

as a Laurent series in $\mathbb{F}_3((t))$. Since

$$2+t+t^3 \ = \ \left(t^3+2t^5+2t^7\right)h(t),$$

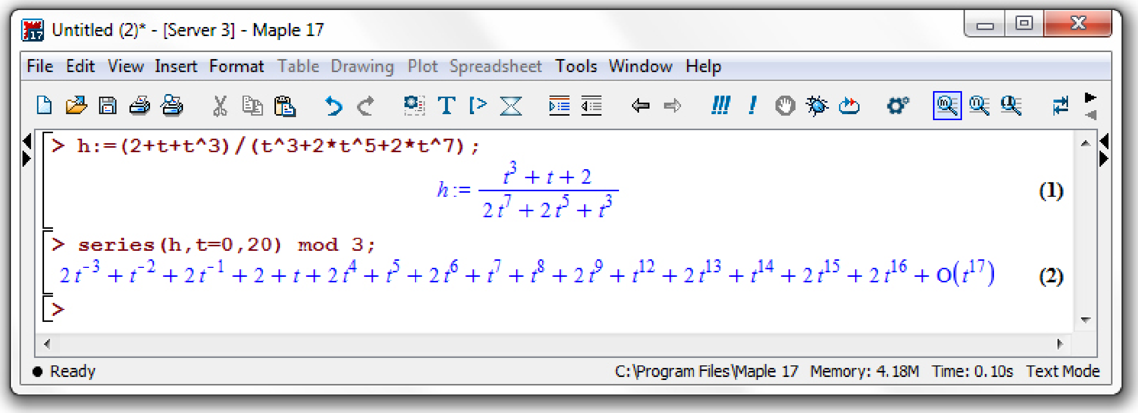
we must have $h(t) = 2t^{-3} + h_{-2}t^{-2} + h_{-1}t^{-1} + h_0 + h_1 t + h_2 t^2 + \cdots$. Now

$$2+t+t^3 \ = \ \left(t^3+2t^5+2t^7\right)\left(2t^{-3} + h_{-2}t^{-2} + h_{-1}t^{-1} + h_0 + h_1 t + h_2 t^2 + h_3 t^3 + \cdots\right),$$

from which we solve $h_{-2}{=}1$, $h_{-1}{=}2$, $h_0{=}2$, $h_1{=}1$, $h_2{=}0$, $h_3{=}0$, $h_4{=}2$, etc. giving us the Laurent series expansion

$$h(t) = 2t^{-3} + t^{-2} + 2t^{-1} + 2 + t + 2t^4 + \cdots \ \in \ \mathbb{F}_3((t)).$$

Let's check this computation using MAPLE®:



Untitled (2)* - [Server 3] - Maple 17
File Edit View Insert Format Table Drawing Plot Spreadsheet Tools Window Help

```
> h:=(2+t+t^3)/(t^3+2*t^5+2*t^7);
```

$$h := \frac{t^3+t+2}{2t^7+2t^5+t^3} \qquad (1)$$

```
> series(h,t=0,20) mod 3;
```

$$2t^{-3}+t^{-2}+2t^{-1}+2+t+2t^4+t^5+2t^6+t^7+t^8+2t^9+t^{12}+2t^{13}+t^{14}+2t^{15}+2t^{16}+\mathrm{O}(t^{17}) \qquad (2)$$

```
>
```

● Ready   C:\Program Files\Maple 17 Memory: 4.18M Time: 0.10s Text Mode

Not every Laurent series represents a rational function, however; i.e. the subring $F(t) \subset F((t))$ is proper. (A subring $S \subseteq R$ is called *proper* if S is a proper subset of R, i.e. there exist elements of R not contained in S.) How do we recognize which Laurent series represent rational functions? And in this case, how do we convert the series representation to a quotient $\frac{f(t)}{g(t)}$ with $f(t), g(t) \in F[t]$ in lowest terms?

Let $r(t) = \sum_{n=k}^{\infty} r_n t^n \in F((t))$, and suppose the coefficients r_n satisfy a recurrence relation of the form $r_n = a_1 r_{n-1} + a_2 r_{n-2} + \cdots + a_m r_{n-m} \ \ldots$ at least for all values of n beyond some point. Then $r(t) \in F(t)$ and we may express $r(t)$ as a rational function by making use of the recurrence formula. This procedure is illustrated well enough by an example, as follows: consider

$$r(t) = \tfrac{1}{2}t^{-1} - \tfrac{3}{4} + \tfrac{5}{8}t - \tfrac{11}{16}t^2 + \tfrac{21}{32}t^3 - \tfrac{43}{64}t^4 + \cdots$$

in which the coefficients satisfy the recurrence formula $r_n = \frac{1}{2}\big(r_{n-2} - r_{n-1}\big)$ for all $n \geq 1$. Let us subtract

$$\begin{array}{rl} r(t) = & \tfrac{1}{2}t^{-1} - \tfrac{3}{4} + \tfrac{5}{8}t - \tfrac{11}{16}t^2 + \tfrac{21}{32}t^3 - \tfrac{43}{64}t^4 + \cdots \\ tr(t) = & \qquad\qquad \tfrac{1}{2} - \tfrac{3}{4}t + \tfrac{5}{8}t^2 - \tfrac{11}{16}t^3 + \tfrac{21}{32}t^4 - \cdots \\ \hline (1-t)r(t) = & \tfrac{1}{2}t^{-1} - \tfrac{5}{4} + \tfrac{11}{8}t - \tfrac{21}{16}t^2 + \tfrac{43}{32}t^3 - \tfrac{85}{64}t^4 + \cdots \end{array}$$

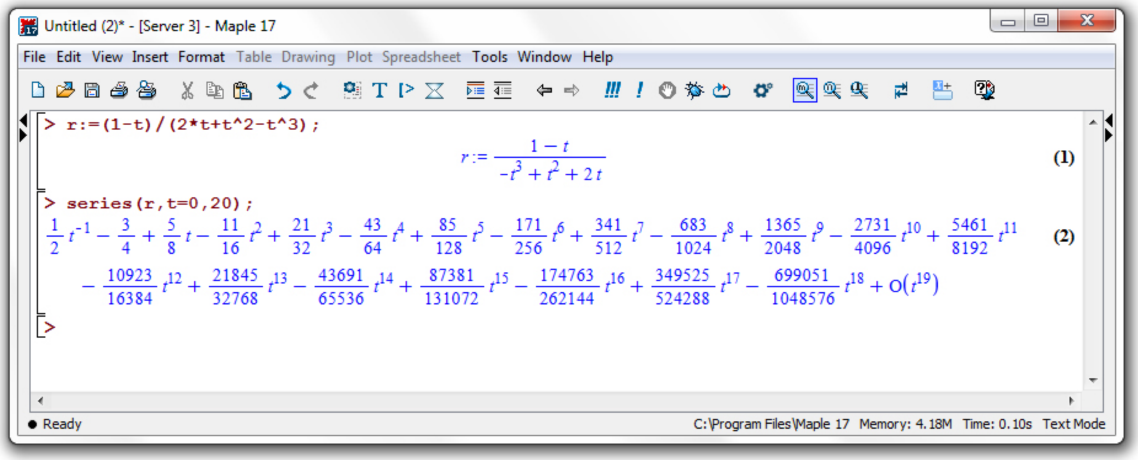
and compare this expansion with the series for $r(t)$. Multiplying by $-\frac{t}{2}$ gives

$$\begin{aligned} \tfrac{1}{2}(t^2 - t)r(t) &= \quad -\tfrac{1}{4} + \tfrac{5}{8}t - \tfrac{11}{16}t^2 + \tfrac{21}{32}t^3 - \tfrac{43}{64}t^4 + \cdots \\ \tfrac{1}{2}(t^2 - t)r(t) + \tfrac{1}{2}t^{-1} - \tfrac{1}{2} &= \tfrac{1}{2}t^{-1} - \tfrac{3}{4} + \tfrac{5}{8}t - \tfrac{11}{16}t^2 + \tfrac{21}{32}t^3 - \tfrac{43}{64}t^4 + \cdots = r(t) \end{aligned}$$

and we can solve the latter equation for $r(t)$. First multiply both sides by $2t$ to get

$$\begin{aligned} (t^3 - t^2)r(t) + 1 - t &= 2tr(t) \\ 1 - t &= (2t + t^2 - t^3)r(t) \\ r(t) &= \frac{1-t}{2t + t^2 - t^3} \end{aligned}$$

Finally, we check our answer using MAPLE®:



Untitled (2)* - [Server 3] - Maple 17
File Edit View Insert Format Table Drawing Plot Spreadsheet Tools Window Help

```
> r:=(1-t)/(2*t+t^2-t^3);
```

$$r := \frac{1-t}{-t^3 + t^2 + 2t} \qquad (1)$$

```
> series(r,t=0,20);
```

$$\frac{1}{2}t^{-1} - \frac{3}{4} + \frac{5}{8}t - \frac{11}{16}t^2 + \frac{21}{32}t^3 - \frac{43}{64}t^4 + \frac{85}{128}t^5 - \frac{171}{256}t^6 + \frac{341}{512}t^7 - \frac{683}{1024}t^8 + \frac{1365}{2048}t^9 - \frac{2731}{4096}t^{10} + \frac{5461}{8192}t^{11} - \frac{10923}{16384}t^{12} + \frac{21845}{32768}t^{13} - \frac{43691}{65536}t^{14} + \frac{87381}{131072}t^{15} - \frac{174763}{262144}t^{16} + \frac{349525}{524288}t^{17} - \frac{699051}{1048576}t^{18} + \mathrm{O}(t^{19}) \qquad (2)$$

```
>
```

Ready
C:\Program Files\Maple 17 Memory: 4.18M Time: 0.10s Text Mode