Manual of the MAGMA package pADICALGEBRAS

Gabor Wiese

24th January 2014

1 Introduction

1.1 Some commutative algebra

We start with a simple case which we will prove directly. Let $\mathbb{T}$ be an *Artinian* algebra, i.e. an algebra in which every descending chain of ideals becomes stationary. Our main example will be finite dimensional algebras over a field. That those are Artinian is obvious, since in every proper inclusion of ideals the dimension diminishes.
For any ideal $\mathfrak{a}$ of $\mathbb{T}$ the sequence $\mathfrak{a}^n$ becomes stationary, i.e. $\mathfrak{a}^n = \mathfrak{a}^{n+1}$ for all n "big enough". Then we will use the notation $\mathfrak{a}^\infty$ for $\mathfrak{a}^n$.

Proposition 1.1. *Let $\mathbb{T}$ be an Artinian ring.*

(a) Every prime ideal of $\mathbb{T}$ is maximal.

(b) There are only finitely many maximal ideals in $\mathbb{T}$.

(c) Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$. It is the only maximal ideal containing $\mathfrak{m}^\infty$.

(d) Let $\mathfrak{m} \neq \mathfrak{n}$ be two maximal ideals. For any $k \in \mathbb{N}$ and $k = \infty$ the ideals $\mathfrak{m}^k$ and $\mathfrak{n}^k$ are coprime.

(e) The Jacobson radical $\bigcap_{\mathfrak{m}\in\mathrm{Spec}(\mathbb{T})} \mathfrak{m}$ is equal to the nilradical and consists of the nilpotent elements.

(f) We have $\bigcap_{\mathfrak{m}\in\mathrm{Spec}(\mathbb{T})} \mathfrak{m}^\infty = (0)$.

(g) (Chinese Remainder Theorem) The natural map

$$\mathbb{T} \xrightarrow{a\mapsto(\dots,a+\mathfrak{m}^\infty,\dots)} \prod_{\mathfrak{m}\in\mathrm{Spec}(\mathbb{T})} \mathbb{T}/\mathfrak{m}^\infty$$

is an isomorphism.

(h) For every maxmimal ideal $\mathfrak{m}$, the ring $\mathbb{T}/\mathfrak{m}^\infty$ is local with maximal ideal $\mathfrak{m}$ and is hence isomorphic to $\mathbb{T}_\mathfrak{m}$, the localisation of $\mathbb{T}$ at $\mathfrak{m}$.

A useful and simple way to rephrase a product decomposition as in (g) is to use idempotents. In concrete terms, the idempotents of $\mathbb{T}$ (as in the proposition) are precisely the elements of the form $(\dots, x_\mathfrak{m}, \dots)$ with $x_\mathfrak{m} \in \{0, 1\} \subseteq \mathbb{T}/\mathfrak{m}^\infty$.

Definition 1.2. *Let $\mathbb{T}$ be a ring. An* idempotent of $\mathbb{T}$ *is an element e that satisfies $e^2 = e$. Two idempotents e, f are* orthogonal *if $ef = 0$. An idempotent e is* primitive, *if $e\mathbb{T}$ is a local ring. A set of idempotents $\{e_1, \ldots, e_n\}$ is said to be* complete *if $1 = \sum_{i=1}^{n} e_i$.*

In concrete terms for $\mathbb{T} = \prod_{\mathfrak{m} \in \mathrm{Spec}(\mathbb{T})} \mathbb{T}/\mathfrak{m}^{\infty}$, a complete set of primitive pairwise orthogonal idempotents is given by

$$(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1, 0), (0, \ldots, 0, 1).$$

We now turn to a more general setting, namely working with a finite algebra $\mathbb{T}$ over a complete local ring instead of a field. We will lift the idempotents of the reduction of $\mathbb{T}$ (for the maximal ideal of the complete local ring) to idempotents of $\mathbb{T}$ by Hensel's lemma. This gives us a proposition very similar to Proposition 1.1.

Proposition 1.3. *Let $\mathcal{O}$ be an integral domain of characteristic zero which is a finitely generated $\mathbb{Z}$-module. Write $\widehat{\mathcal{O}}$ for the completion of $\mathcal{O}$ at a maximal prime of $\mathcal{O}$ and denote by $\mathbb{F}$ the residue field and by K the fraction field of $\widehat{\mathcal{O}}$. Let furthermore $\mathbb{T}$ be a commutative $\mathcal{O}$-algebra which is finitely generated as an $\mathcal{O}$-module. For any ring homomorphism $\mathcal{O} \to S$ write $\mathbb{T}_S$ for $\mathbb{T} \otimes_{\mathcal{O}} S$. Then the following statements hold.*

(a) The Krull dimension of $\mathbb{T}_{\widehat{\mathcal{O}}}$ is less than or equal to 1, i.e. between any prime ideal and any maximal ideal $\mathfrak{p} \subset \mathfrak{m}$ there is no other prime ideal. The maximal ideals of $\mathbb{T}_{\widehat{\mathcal{O}}}$ correspond bijectively under taking pre-images to the maximal ideals of $\mathbb{T}_{\mathbb{F}}$. Primes $\mathfrak{p}$ of height 0 (i.e. those that do not contain any other prime ideal) which are properly contained in a prime of height 1 (i.e. a maximal prime) of $\mathbb{T}_{\widehat{\mathcal{O}}}$ are in bijection with primes of $\mathbb{T}_K$ under extension (i.e. $\mathfrak{p}\mathbb{T}_K$), for which the notation $\mathfrak{p}^e$ will be used.

Under the correspondences, one has

$$\mathbb{T}_{\mathbb{F},\mathfrak{m}} \cong \mathbb{T}_{\widehat{\mathcal{O}},\mathfrak{m}} \otimes_{\widehat{\mathcal{O}}} \mathbb{F}$$

and

$$\mathbb{T}_{\widehat{\mathcal{O}},\mathfrak{p}} \cong \mathbb{T}_{K,\mathfrak{p}^e}.$$

(b) The algebra $\mathbb{T}_{\widehat{\mathcal{O}}}$ decomposes as

$$\mathbb{T}_{\widehat{\mathcal{O}}} \cong \prod_{\mathfrak{m}} \mathbb{T}_{\widehat{\mathcal{O}},\mathfrak{m}},$$

where the product runs over the maximal ideals $\mathfrak{m}$ of $\mathbb{T}_{\widehat{\mathcal{O}}}$.

(c) The algebra $\mathbb{T}_{\mathbb{F}}$ decomposes as

$$\mathbb{T}_{\mathbb{F}} \cong \prod_{\mathfrak{m}} \mathbb{T}_{\mathbb{F},\mathfrak{m}},$$

where the product runs over the maximal ideals $\mathfrak{m}$ of $\mathbb{T}_{\mathbb{F}}$.

(d) The algebra $\mathbb{T}_K$ decomposes as

$$\mathbb{T}_K \cong \prod_{\mathfrak{p}} \mathbb{T}_{K,\mathfrak{p}^e} \cong \prod_{\mathfrak{p}} \mathbb{T}_{\widehat{\mathcal{O}},\mathfrak{p}},$$

where the products run over the minimal prime ideals $\mathfrak{p}$ of $\mathbb{T}_{\widehat{\mathcal{O}}}$ which are contained in a prime ideal of height 1.

1.2 The Newton method

Here we present a special instance of the Newton method. Let R be a ring and $\mathfrak{m}$ an ideal (not necessarily maximal).
Let $f \in R[X]$ be a polynomial. We assume the following: There exist $a \in R$ and a polynomial $b \in R[X]$ such that

$$1 = af(X) + b(X)f'(X).$$

Let further $a_0 \in R$ such that $f(a_0) \in \mathfrak{m}$. For $n \geq 1$ we make the following recursion:

$$a_n := a_{n-1} - f(a_{n-1})b(a_{n-1}).$$

Proposition 1.4. *Suppose $f(a_0) \in \mathfrak{m}^r$ for some $r \geq 1$. Then for all $n \in \mathbb{N}$*

$$f(a_n) \in (\mathfrak{m}^r)^{2^n}.$$

Note that the convergence is exponential.

Proof. Take the Taylor expansion of the polynomial around some x_0:

$$f(x) = f(x_0) + f'(x_0)(x - x_0) + f''(x_0)\frac{(x - x_0)^2}{2!} + \dots.$$

This is a formal equality valid for all x and all x_0.
The proof proceeds by induction on n. The case $n = 0$ is just the assumption. Let us now suppose that $f(a_{n-1}) \in (\mathfrak{m}^r)^{2^{n-1}}$. In the Taylor formula we take $x = a_n = a_{n-1} - f(a_{n-1})b(a_{n-1})$ and $x_0 = a_{n-1}$, yielding

$$\begin{aligned}
f(a_n) &= f(a_{n-1}) - f'(a_{n-1})f(a_{n-1})b(a_{n-1}) + f''(a_{n-1})\frac{f(a_{n-1})^2 b(a_{n-1})^2}{2!} + \dots \\
&= f(a_{n-1})(1 - f'(a_{n-1})b(a_{n-1})) + f''(a_{n-1})\frac{f(a_{n-1})^2 b(a_{n-1})^2}{2!} + \dots \\
&= f(a_{n-1})^2 \cdot a + f''(a_{n-1})\frac{f(a_{n-1})^2 b(a_{n-1})^2}{2!} + \dots \\
&= f(a_{n-1})^2 \cdot \left(a + f''(a_{n-1})\frac{b(a_{n-1})^2}{2!} + \dots\right) \\
&\in \left((\mathfrak{m}^r)^{2^{n-1}}\right)^2 = (\mathfrak{m}^r)^{2^n}.
\end{aligned}$$

This concludes the proof. □

1.3 Lifting idempotents

The main idea of the algorithm is to lift idempotents from an algebra defined over $\mathbb{F}_p$ to $\mathbb{Z}_p$ up to a certain precision. We do this by applying the Newton method explained above.
An idempotent is an element e such that $e^2 = e$. That means, it is a zero of the polynomial $f(X) = X^2 - X$. We'll be working with $R = \mathbb{T}$, a commutative $\mathbb{Z}_p$-algebra which is finitely generated as a $\mathbb{Z}_p$-module (in fact, we'll be giving it as a matrix algebra with generators given as matrices with $\mathbb{Z}$-entries, so that the algebra is known with full precision). The ideal $\mathfrak{m}$ is $p\mathbb{T}$, i.e. the principal ideal

generated by p (if we think in terms of matrix algebras, $\mathfrak{m}$ consists of the matrices all entries of which are divisible by p).
Our input is an idempotent $e_0 \in \mathbb{T}/p\mathbb{T}$, i.e. a root of the polynomial $X^2 - X \in \mathbb{F}_p[X]$. We denote also by e_0 any lift of e_0 to $\mathbb{T}$. Our aim is to enhance e_0 to an element $e_n \in \mathbb{T}$ such that $e_n^2 - e_n \in p^m\mathbb{T}$ for a given m.
We have $f'(X) = 2X - 1$ and

$$1 = -4(X^2 - X) + (2X - 1)(2X - 1), \text{ hence } a = -4 \text{ and } b(X) = 2X - 1.$$

This leads to the recursion for $n \geq 1$:

$$\begin{aligned} e_n &:= e_{n-1} - f(e_{n-1})b(e_{n-1}) \\ &= e_{n-1} - (e_{n-1}^2 - e_{n-1})(2e_{n-1} - 1) \\ &= 3e_{n-1}^2 - 2e_{n-1}^3 \end{aligned}$$

Acknowledgements

I thank Gabi Nebe for having explained this simple algorithmic idempotent lifting to me a long time ago.

2 Usage and Example

The package provides a structure for p-adic algebras, called `pAdicAlgebraFormat`. It is the following record:

```
pAdicAlgebraFormat := recformat <
  p:           RngIntElt, // the p of Z_p
  R:           Any,       // the p-adic ring of given precision
  dim:         RngIntElt, // the dimension of the residual algebra
  deg:         RngIntElt, // degree of the matrix algebra (i.e. number of rows)
  Amod:        Any,       // the full matrix algebra over the residue field
  Aadic:       Any,       // the full matrix algebra over R
  basis:       SeqEnum,   // matrices forming a basis
  adic_coords: Any,       // coordinate function wrt basis
  mod_coords:  Any,       // coordinate function wrt basis mod p
  ipmod:       Any,       // a complete set of orthogonal idempotents for Amod
  ipadic:      Any        // the lifts of ipmod to idempotents in Aadic
>;
```

First attach the packages; the package `ArtinAlgebras` is required by `pAdicAlgebras`.

```
AttachSpec("/home/gabor/Programs/ArtinAlgebras.spec");
AttachSpec("/home/gabor/Programs/pAdicAlgebras.spec");
```

In our example, we create the algebra using integral Hecke operators. Specify level and weight.

```
N := 229; k := 2;
```

Specify the prime at which we work and the desired precision.

```
p := 5; prec := 15;
```

Create the cusp space of modular symbols and compute all Hecke operators up to the Sturm bound.

```
C := CuspidalSubspace(ModularSymbols(N,k,1));
L := [];
for n := 1 to HeckeBound(C) do
  Append(~L, IntegralHeckeOperator(C,n));
end for;
```

Create the p-adic algebra generated by the matrices in the list `L` for the prime `p` and precision `prec`.

```
A := pAdicAlgebra(L,p : prec := prec);
```

Compute the decomposition of `A` as a product of its localisation at the maximal ideals.

```
F := pAdicAlgebraFactors(A);
```

`F` is a list of tuples `<T, phi>`, where `T` is the factor as a p-adic algebra and `phi` is the restriction map from `A` to `T`.
Here are some examples of commands:

```
F[2][1]‘dim;                 // the dimension of the second factor
F[3][2](L[7]);               // the restriction of the Hecke operator L[7]
                             // to the third factor
pAdicMatrixAlgebra(F[3][1]); // the third factor as a matrix algebra
```

Alternatively, one can also calculate one factor after the other, as follows:

```
_compute_adic_idempotents(~A);     // computes the decomposition via idempotents
e := A‘ipadic[1];                  // take the first idempotent
H,phi := pAdicAlgebraFactor(A,e);  // factor corresponding to the idempotent
```