Decomposition of ideals in function fields

Brent Baccala

October 9, 2019

The `decomposition` method in Sage's `FunctionFieldMaximalOrder_global` class uses the "Buchman-Lenstra" algorithm described in [Coh1993] section 6.2. Buchman-Lenstra, however, depends on operations in prime characteristic, and is thus only suitable for number fields and function fields over $\mathbf{F}_p$.

To perform decomposition in characteristic zero, I've developed the alternate algorithm described in this paper, and implemented in the `decomposition` method of Sage's `FunctionFieldMaximalOrder_rational` class.

Given a function field F with a maximal order O and an algebraic field extension F'/F with maximal order $O' \supset O$. We consider a prime ideal P of O, and we wish to find the prime ideals $P'_1, ..., P'_k$ of O' that lie over P, in the sense that $P^e \subset P'_i$, in fact, $P^e = \cap_i P'_i$, i.e, we seek the primary decomposition of P^e.

P^e is the extension of P in O', i.e, the ideal of O' generated by the elements of P. It is not necessarily prime, so the quotient ring $O' \bmod P^e$ is not necessarily either a field or an integral domain. It is, however, an Artinian ring and a finite-dimensional algebra over the field $O \bmod P$. Sage's finite-dimensional algebra subsystem implements[1] the algorithm from Section 7 of [Khuri2004] to find all of the algebra's maximal ideals (all prime ideals of an Artinian ring are also maximal).

$$O \xrightarrow{\phi} O' \xrightarrow{\psi} O' \bmod P^e$$

Thus, we can easily find all maximal ideals of the ring $O' \bmod P^e$. Since the contraction of a maximal ideal is maximal, the maximal ideals of $O' \bmod P^e$ are maximal in O' (via contraction along ψ). Since ψ is surjective, any maximal ideal in O' that contains P^e maps to a maximal ideal in $O' \bmod P^e$ (wikipedia Ideal), so there is a one-to-one relationship between the maximal ideals in $O' \bmod P^e$ and the maximal ideals in O' that contain P^e – exactly what we're looking for.

So, given a maximal ideal P_1 of $O' \bmod P^e$, how can we extract the pertinent information (generators, ramification index, relative degree, β) for its corresponding maximal ideal in O'?

1. **Generators**

   The contraction of P_1 is its preimage under ψ, so a set of generators of the contraction can be formed just by lifting P_1's generators from $O' \bmod P^e$ to O' and appending the generators of P^e.

2. **Ramification Index**

   To see how to compute the ramification index, let's begin by studying how to characterize the ideals of $O' \bmod P^e$

[1] Johan Bosman, personal email, June 19, 2019

Lemma. *P^e consists of all elements in O' with valuation greater than or equal to the ramification index at all places lying over P.*

Proof. O' consists of all elements with valuation greater than or equal to zero at every finite place. P contains at least one element u (any uniformizing variable will do) with valuation equal to the ramification index at *all* places lying over P.

Therefore, given *any* element $e \in O'$ with valuation greater than or equal to the ramification index at *all* places lying over P, we can use the Strong Approximation Theorem to find an element in $f \in O'$ such that fu has the same valuation as e at all places lying over P. Then $\frac{e}{fu} \in O'$ and $e = \frac{e}{fu} fu$ shows that $e \in P^e$. □

[Stich2009] Theorem 1.6.5 (Strong Approximation Theorem). Let $S \subsetneq \mathbb{P}_F$ be a proper subset of $\mathbb{P}_F$ and $P_1, ..., P_r \in S$. Suppose there are given elements $x_1, ..., x_r \in F$ and integers $n_1, ..., n_r \in \mathbb{Z}$. Then there exists an element $x \in F$ such that

$$\nu_{P_i}(x - x_i) = n_i \qquad (i = 1, ..., r), \quad \text{and}$$

$$\nu_P(x) \geq 0 \qquad \forall P \in S \backslash \{P_1, ..., P_r\}.$$

If a function f has valuation greater than or equal to the ramification index at a place P_1, it can be reduced $\text{mod} P^e$ by using the Strong Approximation Theorem to construct a function in P^e with valuation equal to the ramification index at P_1 and valuation greater than f's valuation at all other places over P and adding it to f. Thus $O' \bmod P^e$ contains no functions with valuations greater than the ramification indices.

So, $O' \bmod P^e$ consists of equivalence classes of functions characterized by a tuple of valuations at each place over P, with each valuation no larger than the ramification index at that place. The functions with valuation equal to the ramification index at all places over P are in P^e, and therefore correspond to the zero ideal.

Each prime ideal in $O' \bmod P^e$ is characterized by a tuple like $(1, 0, ..., 0)$ (i.e, a single one and the rest of its elements zero). Squaring it will produce an ideal characterized by $(2, 0, ..., 0)$. Continue raising the prime ideal to higher and higher powers until we've obtained an ideal characterized by $(r, 0, ..., 0)$ (r being the ramification index). Raising the ideal to higher powers will continue producing this same ideal, a manifestation of the Artinian condition guaranteeing that the descending chain of power ideals will stablize.

Thus, we can find the ramification index by raising a prime ideal in $O' \bmod P^e$ to successively higher powers until it stabilizes.

Ex: $y^2 = x$; $P = (x - 1)$.

$P^e = (y^2 - x, x - 1)$ decomposes into $P_1 = (x - 1, y - 1)$ and $P_2 = (x - 1, y + 1)$ with ramification one at both places. Ideals in $O' \bmod P^e$ are characterized by tuples $(0, 0)$, $(1, 0)$, $(0, 1)$, and $(1, 1)$. $(0, 0)$ corresponds to the unit ideal (1), $(1, 0)$ is $(y - 1)$, $(0, 1)$ is $(y + 1)$, and $(1, 1)$ is the zero ideal (0). Our theory suggests that squaring $(y - 1)$ will stabilize it, and we verify that $(y - 1)^2 \equiv -2(y - 1) \bmod P^e$.

Ex: $y^2 = x$; $P = (x)$.

$P^e = (y^2 - x, x)$ decomposes into a single ideal $P_1 = (y)$ with ramification two. Ideals in $O' \bmod P^e$ are characterized by tuples (0), (1), and (2), with (0) corresponding to the unit ideal (1), (1) corresponding to the ideal (y), and (2) corresponding to the zero ideal (0). Our theory leads us to believe that squaring (y) will produce the zero ideal and, indeed, $y^2 \equiv 0 \bmod P^e$.

3. **Relative Degree**

[Stich2009] Definition 3.1.5 defines the relative degree of P' over P as $[F'_{P'} : F_P]$, where F_P (the *residue class field* of P) is defined ([Stich2009] Definition 1.1.14) as O_P/P where O_P is the valuation ring associated with P.

In our notation, F_P is $O \bmod P$ and $F'_{P'}$ is $O' \bmod P_1$. Remember that $O' \bmod P^e$ is a finite-dimensional algebra over F_P. Since

$$F'_{P'} = O' \bmod P_1^c \cong O' \bmod P_e \bmod P_1$$

and we have an F_P-basis for P_1 in $O' \bmod P_e$, we see that the dimension of $F'_{P'}$ over F_P is simply the F_P-dimension of $O' \bmod P_e$ minus the F_P-dimension of P_1. Our finite dimensional algebra code gives us an F_P-basis for P_1, so its dimension is just the length of that basis.

4. $\boldsymbol{\beta}$

   Finally, for computing valuations using [Coh1993] Algorithm 4.8.17, we wish to compute β, an element in O' but not in P^e, and with $\beta P_1 \subseteq P^e$. Working again in $O' \bmod P^e$, we see that β's image is not zero, but multiplying it by each of P_1's generators produces zero.

   Since β is in O' (an O-module), we regard β as a vector in k[x] w.r.t. the basis of O'. As long as at least one element in this vector is not zero, β will not be in P^e. To ensure that $\beta P_1 \subseteq P^e$, multiplying β by each of P_1's generators must produce a vector whose elements are all zero. We can ensure that all this occurs by constructing a matrix in $O \bmod P^e$, and finding a non-zero vector in the matrix's kernel.

References

[Coh1993] Henri Cohen, *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics 138. Springer, 1993.

[Stich2009] Stichtenoth, Henning, *Algebraic function fields and codes*. Vol. 254. Springer Science & Business Media, 2009.

[Khuri2004] Khuri-Makdisi, *Asymptotically Fast Group Operations on Jacobians of General Curves*, 2004. `https://arxiv.org/pdf/math/0409209v2.pdf`