Plans for *p*-adics in Sage

David Roe
with Xavier Caruso and Julian Rüth

Department of Mathematics
University of Calgary

September 5, 2013

Outline

Ramification

Suppose $K/\mathbb{Q}_p$ has degree m. Recall that K is equipped with a unique valuation extending that on $\mathbb{Q}_p$, defined by $v(x) = \frac{1}{m} v_p(\mathrm{Nm}_{K/\mathbb{Q}_p} x)$.

value group – the image of v,

ring of integers – $\mathcal{O}_K = \{x \in K : v(x) \geq 0\}$,

maximal ideal – $\mathfrak{p}_K = \{x \in K : v(x) > 0\} = (\pi_K)$,

residue field – $k = \mathcal{O}_K/\mathfrak{p}_K$.

If L/K is an extension of degree n, write e for the index of the value groups and f for the degree of the residue field extensions.

Theorem

1. $n = ef$
2. *There is a unique subextension M/K that is unramified.*

Krasner's Lemma

Lemma

Let K be a p-adic field and fix an algebraic closure $\bar{K}$. Suppose $f(x) = \prod_{i=1}^{n}(x - \alpha_i) \in K[x]$ is irreducible; set $M = \max_{i,j} v(\alpha_i - \alpha_j)$. We say that $g(x) \in K[x]$ is sufficiently close to $f(x)$ if there is an ordering of the roots $\{\beta_i\}_{i=1}^{n}$ of g with

$$v(\alpha_i - \beta_i) > M.$$

Then such a g is irreducible and $K(\alpha_i) = K(\beta_i)$ for all i.

Thus we may talk about *the* field extension defined by a polynomial f, even if we only have a finite approximation to f.

Question

Is there an easy way of rephrasing this condition in terms of the coefficients of f and g?

Unramified Extensions

Krasner's Lemma implies that two unramified extensions of K are isomorphic if their defining polynomials are congruent modulo $\mathfrak{p}_K$, reflecting the equivalence of categories defined by the Witt vectors functor between finite extensions of k and finite unramified extensions of K.

Totally Ramified Extensions

If L/K is totally ramified then the minimal polynomial of a uniformizer will be Eisenstein. Conversely, suppose that $f = \pi_K(f_0 + \cdots + f_{n-1}x^{n-1}) + x^n \in K[x]$ is Eisenstein, and model elements of $L = K[x]/(f)$ as polynomials in x. The image of x in this quotient is a uniformizer, and one can easily compute the valuation of an element from the valuations of its coefficients. Moreover, scaling elements by powers of π_L is aided by the fact that the uniformizer is so simple.

Equality testing is also compromised, since extra p-adic digits may be required to store all distinct elements modulo π_L^c.

Question

Are there examples (e.g. cyclotomic fields) where the benefits of using a non-Eisenstein polynomial outweigh the downsides?

General Extensions

In general, we can decompose an extension into an unramified extension followed by a totally ramified extension, and thus we can represent elements as polynomials in two variables, a variable generating the unramified piece, and the uniformizer.

Question

With f arbitrary, suppose we're given a uniformizer in $K[x]/(f)$. What impediments are there to using this representation?

Precision

We will model a polynomial over $\mathbb{Z}_p$ as a polynomial $P \in \mathbb{Z}[x]$ together with a precision structure. Different precision structures:

- **flat** – every coefficient has the same absolute precision,
- **newton** – the precision of the error term is given by a convex polygon,
- **jagged** – each coefficient has its own individual precision.

We can perform arithmetic operations separately on the approximating polynomials and the precision structures.

Precision for Evaluation

Here we consider the function $f : K[X] \times K \to K, (P, a) \mapsto P(a)$.
We have:

$$\begin{aligned}(P + dP)(a + da) &= P(a + da) + dP(a + da) \\ &= P(a) + P'(a)da + dP(a) + \text{(terms of order} \geq 2).\end{aligned}$$

Hence, the differential of f is given by:

$$df_{(P,a)}(dP, da) = dP(a) + P'(a)da.$$

Precision for Euclidean division

Let d be a positive integer. Let $K_{=d}[X]$ denote the open subset of $K_{<d+1}$ of polynomials of degree exactly d. It is apparently a differentiable variety (of dimension $d+1$) over K. Consider the function $f : K[X] \times K_d[X] \to K[X] \times K_{<d}[X], (A, B) \mapsto (Q, R)$ where Q and R denote respectively the quotient and the reminder in the euclidean division of A by B. The differential of f can be computed as follows. From $(A + dA) = (B + dB)(Q + dQ) + (R + dR)$ we get

$$dA - dB \cdot Q = B \cdot dQ + dR.$$

Hence $df_{(A,B)}(dA, dB) = (dQ, dR)$ where dQ and dR are the quotient and the reminder in the euclidean division of $dA - dB \cdot Q$ by B.

Let d be a positive integer. Suppose we are given $P \in K_{<d}[X]$ and $a \in K$ a simple root of P. Then we can follow this root on a neighbourhood of P: there exists a continuous map $f : U \to K$ (where U is an open subset containing P) such that $Q(f(Q)) = 0$ for all $Q \in U$. Actually, f is also differentiable at P and we can compute its differential thanks to the following computation:

$$0 = (P+dP)(a+da) = P(a)+dP(a)+P'(a)da+(\text{terms of order} \geq 2).$$

We find:

$$df_P(dP) = -\frac{dP(a)}{P'(a)}.$$

Precision for Factoring

Suppose $P \in K[x]$ has a newton precision with nonzero constant term, and that Q and R are high precision polynomials with $P = QR$ up to the precision dP of P. We would like to define a meaningful notion of the precision of Q and R. Since Q and R have high precision and P has a nonzero constant term, Q and R have well defined Newton polygons, $N(P)$ and $N(R)$. Suppose we introduced precisions, $Q + dQ$ and $R + dR$. Then the precision of the product is $Q \cdot dR + dQ \cdot R$. The precision dR should be maximal so that the newton polygon $N(Q \cdot dR)$ is below $N(dP)$.

Question

This maximality constraint does not define dR uniquely. How should we choose among different precisions dR?

Non-unique precision for factoring

Suppose $dP = p^10 + p^8x + p^8x^2 + p^8x^3 + p^10$ and $Q = p + x + px^2$. Then

$$dR = p^7(p^2 + x + p^2x^2)$$

and

$$dR = p^8(1 + x + x^2)$$

are both maximal choices for dR.

Completions

Suppose $p \in \mathbb{Z}$ is prime and K is a number field defined by a polynomial $f \in \mathbb{Q}[x]$. We would like to find the completions of K at primes above p. This is equivalent to factoring $f = \prod_i f_i$ in $\mathbb{Q}_p[x]$. The inclusion $K \hookrightarrow K_i$ of $K = \mathbb{Q}[x]/(f)$ into the completion $K_i = \mathbb{Q}_p[x]/(f_i)$ is the obvious one.

Global questions

Once we have completions $K \hookrightarrow K_i$, we may ask global questions.

Question (Weak Approximation)

Suppose we're given a finite set S of primes in K and elements $\alpha_\nu \in K_\nu$ for $\nu \in S$. How can we find $\alpha \in K$ so that the image of α in K_ν is α_ν?