Newton theorem

Bassel Mannaa

bassel@chalmers.se

University of Gothenburg

Nov 12, 2010

Preliminaries

Problem

For a field K, Find the linear factors of a monic polynomial in $K[X][Y]$.

- Roots may have coefficient in some extension $F \backslash K$ e.g.

  $Y^2 + X^2 = (Y - \imath X)(Y + \imath X)$

- Roots may be power series rather than polynomials e.g.

  $Y^2+X^2-1 = (Y+1-\frac{1}{2}X^2-\frac{1}{8}X^4+...)(Y-1+\frac{1}{2}X^2+\frac{1}{8}X^4+...)$

- Exponents in the roots may be rational e.g.

  $Y^2 - X = (Y - X^{1/2})(Y + X^{1/2})$

Hensel's lemma

Theorem (Hensel's lemma)

For R a commutative ring. Given

$$F(X,Y) = Y^n + a_1(X)Y^{n-1} + ... + a_n(X) \in R[[X]][Y],$$

monic of degree n.

$G_0, H_0 \in R[Y]$ *monic of degrees $r, s > 0$ resp. with $r + s = n$*

$G^*, H^* \in R[Y]$ *such that $F(0,Y) = G_0H_0$ and*

$G_0H^* + H_0G^* = 1$.

Then there exist monic $G(X,Y), H(X,Y) \in R[[X]][Y]$ of degrees r, s resp. such that $G(0,Y) = G_0$, $H(0,Y) = H_0$ and

$F(X,Y) = G(X,Y)H(X,Y)$.

Newton Theorem

Theorem (Newton Theorem)

For K algebraically closed with zero characteristic, given

$$F(X,Y) = Y^n + a_1(X)\, Y^{n-1} + ... + a_n(X) \in K[[X]][Y]$$

monic of degree n such that $\exists A, B \in K((X))[Y].\ AF + BF_Y = 1$.

Then there exist $m \in \mathbb{N}^+$ such that

$$F(X,Y) = \prod_{i=1}^{n} \left(Y - \eta_i(X^{1/m})\right) \quad , \eta_i(X^{1/m}) \in K[[X^{1/m}]]$$

Abhyankar's proof

Outline

- Find two coprime factors of $F(0, Y)$.
- Use Hensel's lemma to lift those to factors of $F(X, Y)$ in $K[[X]][Y]$.
- Inductively repeat the process for the obtained factors.

Modifying the roots

Sometimes $F(0, Y)$ doesn't have two coprime factors For example:

$F(X, Y) = Y^2 + 2Y + YX + 1$. We have

$F(0, Y) = Y^2 + 2Y + 1 = (Y + 1)^2$.

generally

$$(Y + a)^n = \begin{cases} Y^n + naY^{n-1} + ... + a^n & a \neq 0 \\ Y^n & a = 0 \end{cases}$$

Modifying the roots

Killing $(n-1)^{th}$ coefficient (Adding to the roots)

Letting $Y = Z - \frac{a_1(X)}{n}$ in $F(X,Y)$ we get

$\tilde{F}(X,Z) = Z^n + \tilde{a_1}(X)Z^{n-1} + ... + \tilde{a_n}(X)$ with $\tilde{a_1}(X) = 0$

Example

In $Y^2 + 2Y + YX + 1$ we let $Y = Z - \frac{(X+2)}{2}$

$F(X,Y) = \tilde{F}(X,Z) = Z^2 - \frac{X^2}{2} - 2X - 1$

$\tilde{F}(0,Z) = Z^2 - 1 = (Z-1)(Z+1)$

Modifying the roots

Consider $F(X,Y) = Y^2 + Y(X-2) + 2$.

- We kill the $(n-1)^{th}$ coefficient to get

  $F_1(X,Z) = Z^2 - \frac{1}{2}X^2 + 2X$ with $F_1(0,Z) = Z^2$.

Multiplying the roots

If we multiply the roots of $\tilde{F}(X,Z) = \prod_i^n (Z - r_i)$ by b we get

$$\prod_i^n (Z - br_i) = b^n \tilde{F}(X, b^{-1}Z) =$$

$$Z^n + a_1(\tilde{X})bZ^{n-1} + ... + a_i(\tilde{X})b^i Z^{n-i} + ... + a_n(\tilde{X})b^n$$

Modifying the roots

We multiply the roots of $\tilde{F}$ by X^{-d} to get another polynomial

$$F^*(X,Z) = X^{-dn}\tilde{F}(X, X^d Z) = Z^n + \sum_{i=1}^{n} \tilde{a}_i(X) X^{-di} Z^{n-i}$$

We choose d such that

- The coefficients are power series (no negative exponent of X).
- One of the coeff has a constant term, i.e. $F_2(0,Z) \neq Z^n$.

i.e. For all i, $di \leqslant \operatorname{ord} a_i$ and for some j, $dj = \operatorname{ord} a_j$. Hence, we take $d = \min_{i=1}^{n} \left(\frac{\operatorname{ord} a_i(X)}{i}\right)$.

Modifying the roots

Consider $F_3 = Z^3 + ZX - \frac{1}{2}X^2 + 2X$. For which $d = 1/3$.

Multiplying the roots we get

$F_4 = X^{-1}F_3(X, X^{1/3}Z) = Z^3 + X^{\frac{2}{3}}Z - \frac{1}{2}X + 2.$

To Fix the rational exponents in the coefficients, we take $W^3 = X$.

Hence $F_4 = W^{-3}F_3(W^3, WY) = Y^3 + W^2Y - \frac{1}{2}W + 2.$

In general if $d = \dfrac{\lambda}{\mu}$ we take $W^\mu = X$ and

$$F^*(W, Z) = W^{-\lambda n}\tilde{F}(W^\mu, W^\lambda Z) = Z^n + \sum_{i=1}^{n} a_i^*(W)W^{-\lambda i}Z^{n-i}$$

Modifying the roots

Does $d = \min_{i=1}^{n} \left(\frac{\operatorname{ord} a_i(X)}{i} \right)$ exist?

Recall that the coefficients are *power series* in X over K. Consider the zero power series $0 \in K[[X]]$. The computation $\operatorname{ord}(0)$ will not terminate.

- Abhyankar uses the law of excluded middle : In case $F = Y^n$ we are done, otherwise we proceed with multiplication of roots.

Apartness relation

Definition

For a set S. A Relation $\#$ on S is an *apartness* if

AX.1 $\neg(x \# y) \leftrightarrow x = y$

AX.2 $x \# y \rightarrow x \# z \vee y \# z$

On a *nontrivial* commutative ring R

AX.3 $x + y \# w + z \rightarrow x \# w \vee y \# z$

AX.4 $xy \# wz \rightarrow x \# w \vee y \# z$

AX.5 $1 \# 0$

For $a, b \in R[[X]]$ for R discrete $a \# b \leftrightarrow \exists i \in \mathbb{N}.\ a(i) \neq b(i)$.

Apartness lemma for Newton theorem

Lemma

For a polynomial $F \in R[Y]$ of degree n, where $(R, \#)$ is a commutative ring with apartness relation. Let F_Y be the derivative of F. If there exist $A, B \in R[Y]$ and $R \ni C \# 0$ such that $AF + BF_Y = C$ then $\forall n > 1.\ F \# Y^n$.

Note

If $AF + BF_Y = C$ holds for $F, A, B \in R[Y], C \in R$ then it holds for any $G \mid F$. Hence, the lemma holds with the inductive application of Hensel's lemma.

Algebraic closure: Kronecker's Model

Preliminaries

- For $f(X) \in K[X]$ irreducible, $K(\alpha) = K[X]/(f)$ is a field.

  Moreover,

- α the image of X under $\pi : K[X] \to K[X]/(f)$ is a root of $f(Y) \in K(\alpha)[Y]$.

Algebraic closure: Kronecker's Model

Kronecker's construction

$K[X] \ni F = p_1^{e_1} ... p_n^{e_n}$ let $K(\alpha) = K[X]/(p_1)$

$K(\alpha)[X] \ni F = (X - \alpha)F_2.$

Doing this inductively we extend the model of the field K to a bigger model of a field over which the F factors linearly (splits).

- No *general* method for factorization of polynomials over an explicitly given field (Van Der Waerden,1930).
- Factorization is computationally expensive.

Algebraic closure: Dynamic construction (Duval et al)

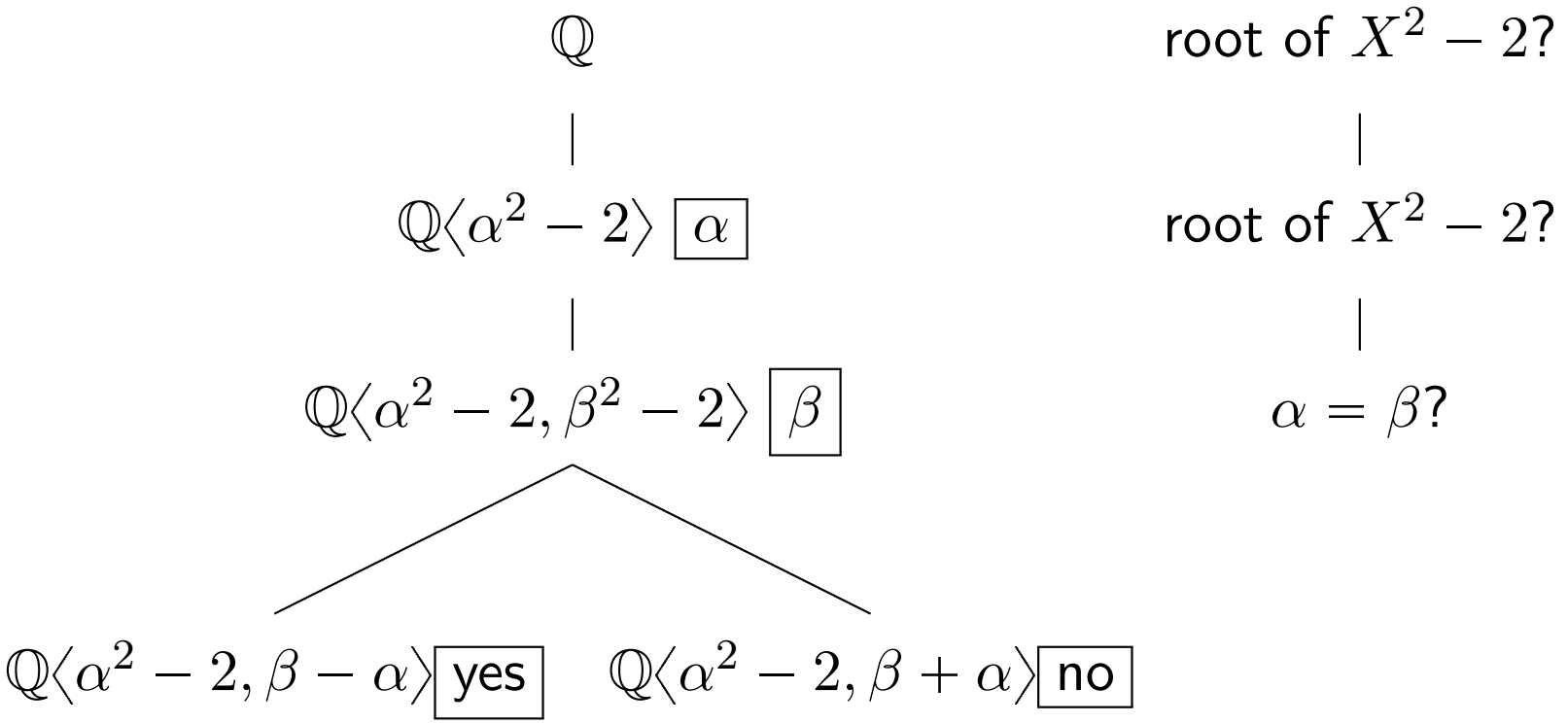
The idea

For $p, q \in K[X]$ $(\deg(p) > 0)$

- p and q are coprime $(rp + sq = 1 \in K[X])$, then q is a unit in $K[X]/(p)$ with inverse r.
- $p \mid q$, then q is 0 in $K[X]/(p)$.
- If p is square free, then q is 0 in $K[X]/(\gcd(p, q))$ and unit in $K[X]/\left(\frac{p}{\gcd(p,q)}\right)$.

Algebraic closure: Dynamic construction

Example



Algebraic closure: Dynamic construction

Example

$$\mathbb{Q} \qquad \text{root of } X+1?$$

$$\mid \qquad \mid$$

$$\mathbb{Q}\langle \alpha+1 \rangle \boxed{\alpha} \qquad \text{root of } X^2+1?$$

$$\mid \qquad \mid$$

$$\mathbb{Q}\langle \alpha+1, \beta^2+1 \rangle \boxed{\beta} \qquad \alpha = \beta^2?$$

$$\mid$$

$$\mathbb{Q}\langle \alpha+1, \beta^2+1 \rangle \boxed{\text{yes}}$$

Algebraic closure: Dynamic construction

Dynamic construction

Construction of the closure L is *in a sense* delayed, the axiom schemata

$$\forall a \in L.\ a = 0 \vee \exists b.\ a\ b = 1$$

$$\forall q(X) \in L[X].\ \deg q \geqslant 1 \to \exists \alpha \in L.\ \ q(\alpha) = 0$$

are satisfied instance by instance (*on demand*).

In Haskell

- Type of algebraic closure : $K[X_1, ..., X_n, ...]$

  Internally: $K[X_1, ..., X_n]$ for some n.

- We have a state

  $[p_1(X_1), p_2(X_1, X_2), ...]$ where

  $p_i(X_1, .., X_i) \in K[X_1, ..., X_{i-1}][X_i]$ such that each

  $p_i(X_1, .., X_i)$ is monic in X_i and square free in

  $(K[X_1, .., X_{i-1}]/(p_{i-1}))[X_i]$.

- Computation is done monadically (state wise) through the

  state monad

  ```
  newtype State st result = ST st -> [(st,result)]
  ```

Examples

- `Y^6 + X^6 + 3 X^2 Y^4 + 3 X^4 Y^2 - 4 X^2 Y^2`

  `State: a^4-4=0,b+4/5a=0,c=0,d^2-1/4=0,a_0^2+a^2=0`

  `Result: (Y-aX^1/2+3/16a^3X^3/2+ ...)`

  `(Y+aX^1/2-3/16a^3X^3/2+ ...)`

  `(Y-dX^2+ ...) (Y+dX^2+ ...)`

  `(Y-a_0X^1/2-3/16a^2a_0X^3/2+ ...)`

  `(Y+a_0X^1/2+3/16a^2a_0X^3/2+ ...)`

- `X^5 - (1/2) X^3 Y + X^2 Y^2 - (1/2) X Y^3 + Y^5`

  `State: a=0,b-1/3=0,c^2-4=0,d^2-1/2=0`

  `Result: (Y-X-cX^3/2-3X^2-65/8cX^5/2-54X^3+ ...)`

  `(Y-X+cX^3/2-3X^2+65/8cX^5/2-54X^3+ ...)`

  `(Y-2X^2-8X^3+ ...)`

  `(Y-dX^1/2+X+2dX^3/2+4X^2+20dX^5/2+58X^3+ ...)`

  `(Y+dX^1/2+X-2dX^3/2+4X^2-20dX^5/2+58X^3+ ...)`

- `-X^3 + X^4- 2X^2Y- XY^2+ 2XY^4+ Y^5`

  `State: a=0,b^2-1=0,c^3-1=0,d^2+3/4c^2=0`

  `Result: (Y+X+ ...) (Y+X+ ...) (Y-cX^1/3+ ...)`

  `(Y+(-d+1/2c)X^1/3+ ...) (Y+(d+1/2c)X^1/3+ ...)`