Computerpraktikum

Block I

Heben von Nullstellen

Matthias Künzer

Universität Stuttgart

18. November 2011

Inhalt

1 Magma **2**

2 Nullstellen modulo p von rational irreduziblen Polynomen **3**

3 Nullstellen modulo p^k – Hebungsbäume **4**

4 p-adische Zahlen **8**

5 Newton-Hensel-Verfahren **10**
5.1 Taylor 10
5.2 Existenzfragen 11
5.3 Eindeutigkeitsfragen 14

6 Henselbare Nullstellen in den Hebungsbäumen **15**

7 Zerlegung in irreduzible Faktoren in $\mathbf{Z}_p[X]$ **21**

A Hensel-Koch-Verfahren **27**
A.1 Diskriminante 27
A.2 Resultante 27

Vorwort

In diesem Drittel des Computerpraktikums soll der Frage nachgegangen werden, ob und wie man Nullstellen eines Polynoms $f(X) \in \mathbf{Z}[X]$ modulo p zu Nullstellen modulo p^k für $k \geqslant 1$ heben kann. Hierbei sollen p-adische Zahlen helfen, das Verhalten zu verstehen.

Für Hinweise auf Fehler und Unklarheiten und mögliche Verbesserungen bin ich dankbar.

Ein Dank geht an Markus Kirschmer, Gabriele Nebe und Bernd Souvignier für hilfreiche Kommentare; die Verantwortung bleibt bei mir. Ein Dank geht an Jana Franz, Juliane Deissler und weitere Studenten für Korrekturen.

Stuttgart, den 22.11.2010

Matthias Künzer

1 Magma

Wir verwenden das Computeralgebra-System Magma.

Das Handbuch findet sich unter `magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`.

Ein Magma-Online-Rechner findet sich unter `http://magma.maths.usyd.edu.au/calc/`.

Am Rechner wird Magma in einer Shell mittels `magma` aufgerufen. Darin wird die Hilfe e.g. für den Begriff "Integers" mit `?Integers` aufgerufen.

2 Nullstellen modulo p von rational irreduziblen Polynomen

Für $a, b \in \mathbf{Z}$ und $m \in \mathbf{Z}$ schreiben wir $a \equiv_m b$ für $a - b \in m\mathbf{Z}$.

Beachte, daß für $a, b \in \mathbf{Z}$, $f(X) \in \mathbf{Z}[X]$ und $m \in \mathbf{Z}$ aus $a \equiv_m b$ folgt, daß $f(a) \equiv_m f(b)$.

Ferner schreiben wir für $a \in \mathbf{Z}$ kurz $\mathbf{Z}/a := \mathbf{Z}/a\mathbf{Z}$.

Sei p prim.

Sei $f(X) \in \mathbf{Z}[X]$ ein gegebenes Polynom mit ganzzahligen Koeffizienten. Sei $f(X)$ in $\mathbf{Z}[X]$ (oder, äquivalent, in $\mathbf{Q}[X]$) nicht nichttrivial in Faktoren zerlegbar, kurz, *rational irreduzibel.*

Dennoch kann es $a \in \mathbf{Z}$ mit $f(a) \equiv_p 0$ geben. Diesenfalls sagen wir, a ist eine *Nullstelle von $f(X)$ in $\mathbf{Z}/p$*; oder eine *Nullstelle modulo p*; oder eine *modulare Nullstelle.*

Diese Eigenschaft hängt nur von der Restklasse von a in $\mathbf{Z}/p$ ab.

Beispiel. Das Polynom $u_1(X) := X^2 + X + 1 \in \mathbf{Z}[X]$ ist mangels Nullstellen rational irreduzibel, hat aber die Nullstelle 1 in $\mathbf{Z}/3$, da $u_1(1) = 3 \equiv_3 0$.

Beispiel. Das Polynom $u_2(X) := X^4 + X + 1 \in \mathbf{Z}[X]$ ist rational irreduzibel, hat aber die Nullstelle 3 in $\mathbf{Z}/5$.

```
Z := Integers();
Q := Rationals();
P<X> := PolynomialRing(Q);
u := X^4 + X + 1;
IsIrreducible(u);
// Auswertung einzeln:
Evaluate(u,3);
// Oder systematischer:
for i in [1..5] do print Evaluate(u,i); end for;
// Gleich zerlegt:
for i in [1..10] do print Factorisation(Z!Evaluate(u,i)); end for;
```

Suche Beispiele!

Verschiedene Arbeitsgruppen sollten weitgehend verschiedene Beispiele haben.

3 Nullstellen modulo p^k – Hebungsbäume

Sei $f(X) \in \mathbf{Z}[X]$ ein rational irreduzibles Polynom. Sei p prim.

Sei $k \geqslant 1$. Sei $a \in \mathbf{Z}$. Ist $f(a) \equiv_{p^k} 0$, so sagen wir, a ist eine *Nullstelle von* $f(X)$ *in* $\mathbf{Z}/p^k$ oder *modulo* p^k.

Sei $a \in \mathbf{Z}$ eine Nullstelle von $f(X)$ modulo p^k. Sei $\ell \geqslant 1$. Ist $b \in \mathbf{Z}$ eine Nullstelle von $f(X)$ modulo $p^{k+\ell}$ und ist $b \equiv_{p^k} a$, dann sagen wir, daß b *eine Nullstelle modulo* $p^{k+\ell}$ *ist, die die Nullstelle* a *modulo* p^k *hebt.*

Wir zeichnen einen *Hebungsbaum* wie folgt.

In der Ebene 1 werden alle Nullstellen in $\mathbf{Z}/p$ eingetragen, mit Repräsentanten in $[0, p-1]$ ([1]).

In der darüberliegenden Ebene 2 werden alle Nullstellen in $\mathbf{Z}/p^2$ eingetragen, mit Repräsentanten in $[0, p^2-1]$. Reduziert eine solche Nullstelle zu einer darunter eingetragenen Nullstelle in $\mathbf{Z}/p$, so werden sie durch eine Kante verbunden.

In der darüberliegenden Ebene 3 werden alle Nullstellen in $\mathbf{Z}/p^3$ eingetragen, mit Repräsentanten in $[0, p^3-1]$. Reduziert eine solche Nullstelle zu einer darunter eingetragenen Nullstelle in $\mathbf{Z}/p^2$, so werden sie durch eine Kante verbunden.

In der darüberliegenden Ebene 4 werden alle Nullstellen in $\mathbf{Z}/p^4$ eingetragen, mit Repräsentanten in $[0, p^4-1]$. Reduziert eine solche Nullstelle zu einer darunter eingetragenen Nullstelle in $\mathbf{Z}/p^3$, so werden sie durch eine Kante verbunden.

Usf.

```
Z := Integers();
Q := Rationals();
P<X> := PolynomialRing(Q);
p := 5;
u := X^4 - 4*X + 1;
for k in [1..5] do
 print "Ebene:", k;
 for i in [0..p^k-1] do
  if Z!Evaluate(u,i) mod p^k eq 0 then print(i); end if;
 end for;
end for;
```

[1] Oder, wahlweise, in $[-(p-1)/2, +(p-1)/2]$.

Oder mit eingebauter Suche nach interessanten Beispielen:

```
Z := Integers();
Q := Rationals();
P<X> := PolynomialRing(Q);
p := 5; height := 5;
for a in [-3..3] do for b in [-3..3] do for c in [-3..3] do for d in [-3..3] do
 u := X^6 + a*X^3 + b*X^2 + c*X + d;
 if IsIrreducible(u) then
  tree := [];
  for k in [1..height] do
   for i in [0..p^k-1] do
    if Z!Evaluate(u,i) mod p^k eq 0 then Append(~tree,<k,i>); end if;
   end for;
  end for;
  if #[x : x in tree | x[1] eq 1] lt #[x : x in tree | x[1] eq 2] then
   print "a =", a, "b =", b, "c =", c, "d =", d, tree;
  end if;
 end if;
end for; end for; end for; end for;
```

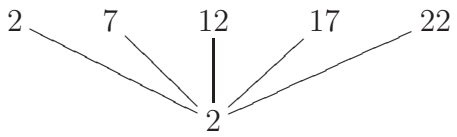
Vorstehendes Programm ist nicht optimal, da die Bäume immer komplett angelegt werden und dann erst anhand der Ebenen 1 und 2 entschieden wird, ob sie interessant sind.

Beispiel. Sei $u_1(X) := X^2 + X + 1$. Sei $p = 3$. Der Hebungsbaum hat nur den Eintrag 1 in Ebene 1.

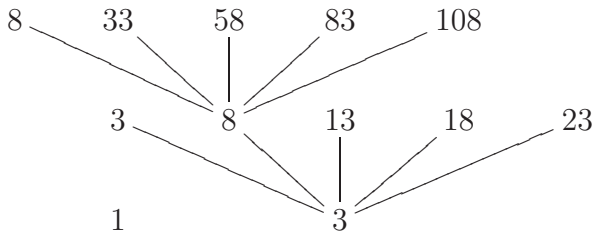
1

Beispiel. Sei $u_2(X) := X^4 + X + 1$. Sei $p = 5$. Wir erhalten folgenden Hebungsbaum.

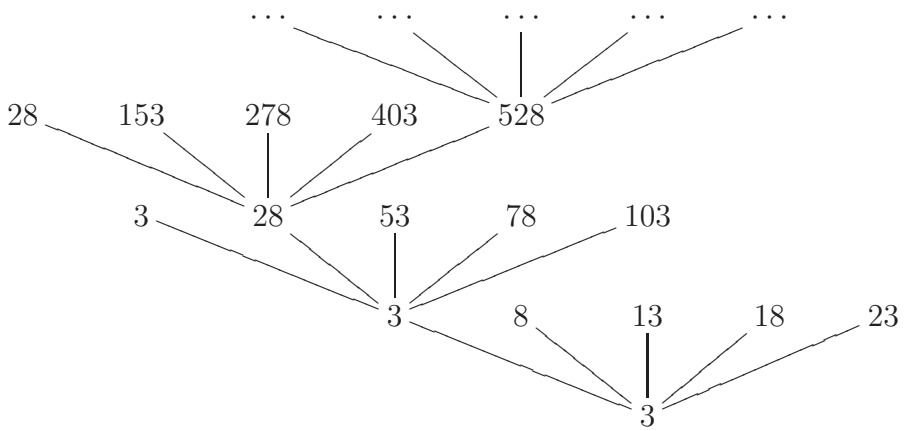
Beispiel. Sei $u_3(X) := X^4 + 3X + 3$. Sei $p = 5$. Wir erhalten folgenden Hebungsbaum.



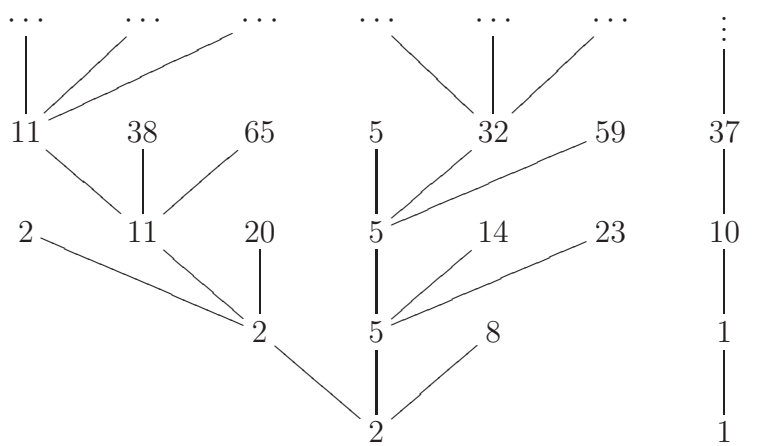
Beispiel. Sei $u_4(X) := X^4 - 3X^3 - 3X^2 + X - 1$. Sei $p = 5$. Wir erhalten folgenden Hebungsbaum.



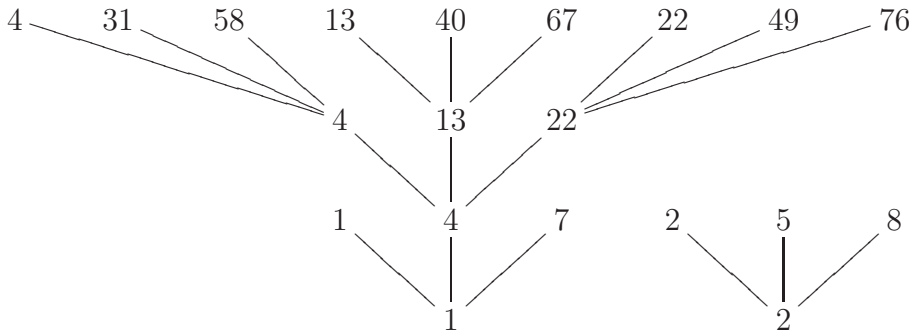
Beispiel. Sei $u_5(X) := X^6 - 6X^3 - 6X^2 - 5X + 2$. Sei $p = 5$. Wir erhalten folgenden Hebungsbaum.



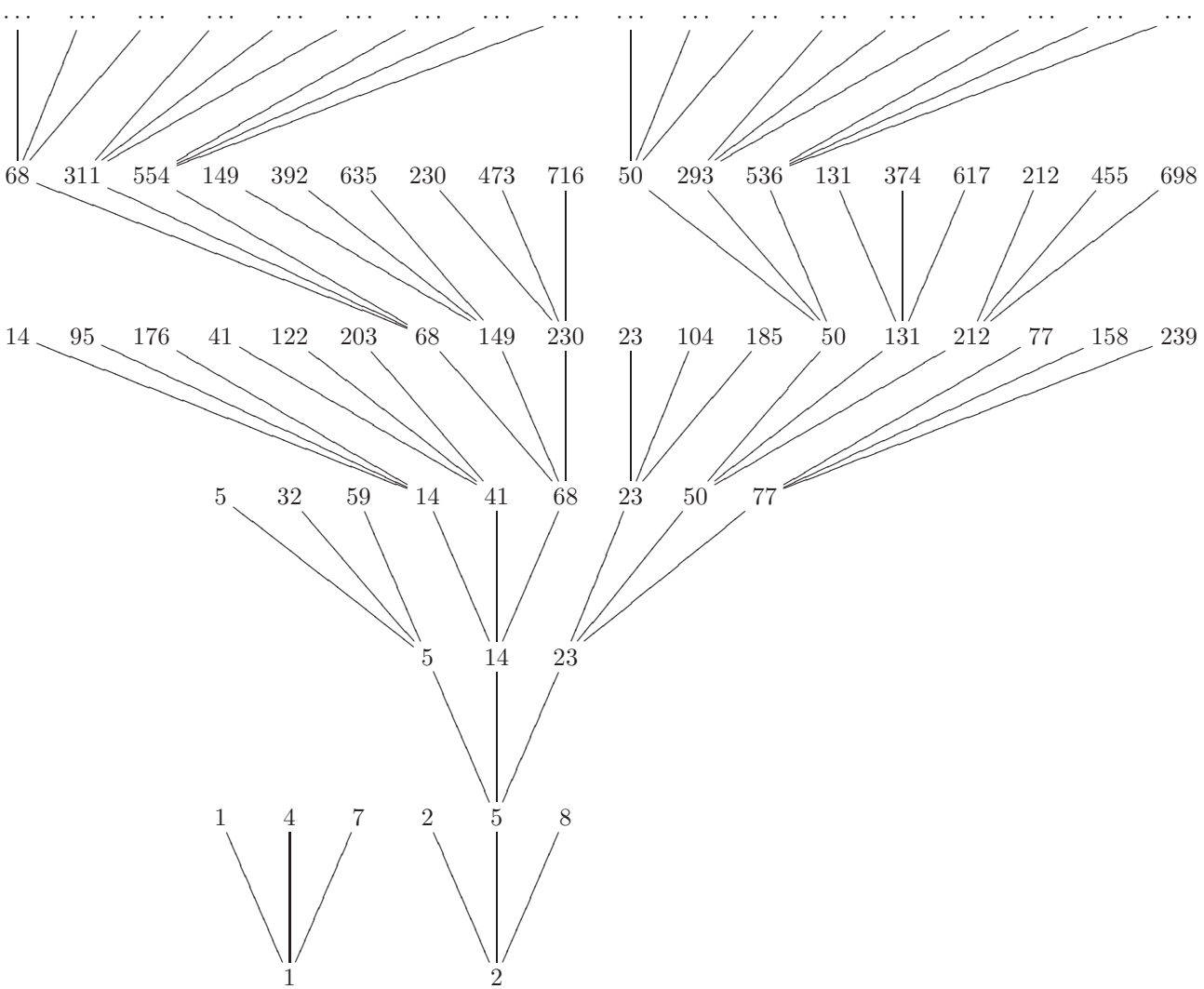
Beispiel. Sei $u_6(X) := X^3+X^2-X+17$. Sei $p = 3$. Wir erhalten folgenden Hebungsbaum.



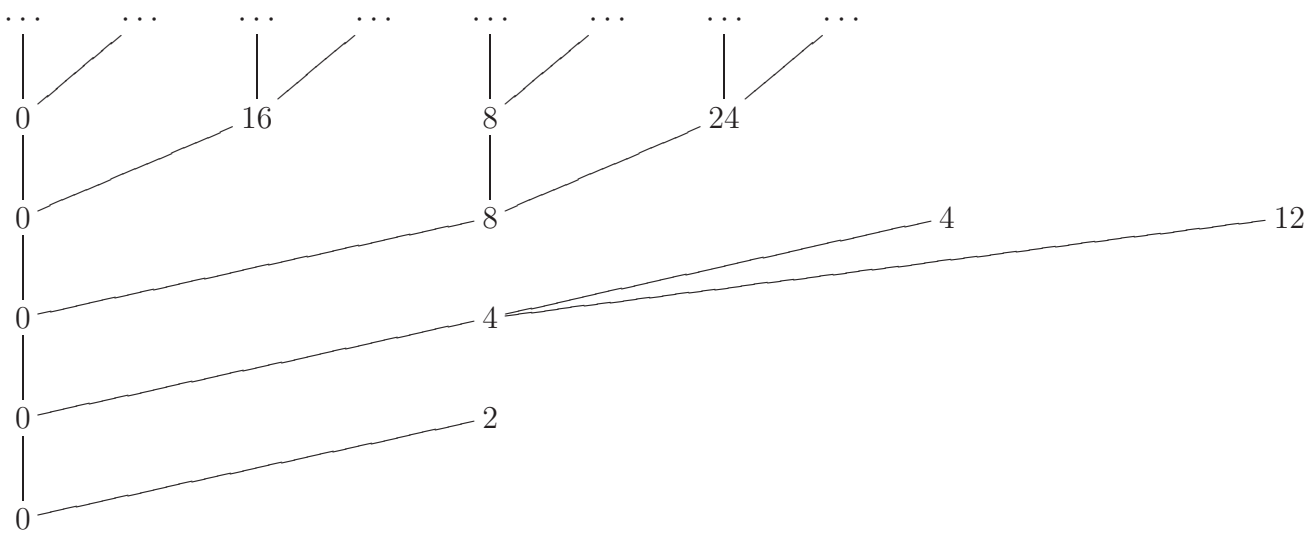
Beispiel. Sei $u_7(X) := X^6 - 4X^4 - 6X^3 + 5X^2 - 3X - 2$. Sei $p = 3$. Wir erhalten folgenden Hebungsbaum.



Beispiel. Sei $u_8(X) := X^6 - X^4 - 6X^3 - 4X^2 + 6X - 5$. Sei $p = 3$. Wir erhalten folgenden Hebungsbaum.



Nicht-Beispiel. Sei $u_9(X) := X^2$, was natürlich nicht rational irreduzibel ist. Sei $p = 2$. Wir erhalten folgenden Hebungsbaum.



Erstelle Hebungsbäume für die in §2 selbstgefundenen Beispiele (oder bessere)!

Das Ziel des Praktikums ist es, möglichst viel über diese Bäume in Erfahrung zu bringen.

4 p-adische Zahlen

Sei p prim.

Sei

$$\mathbf{Z}_p \;:=\; \left\{(a_{[i]} + p^i\mathbf{Z})_{i\geqslant 1} \;:\; a_{[i]} \in \mathbf{Z} \text{ mit } a_{[i+1]} \equiv_{p^i} a_{[i]} \text{ für } i \geqslant 1\right\} \;\subseteq\; \prod_{i\geqslant 1} \mathbf{Z}/p^i \;.$$

Die eckigen Klammern dienen dabei nur der Kenntlichmachung einer ganzen Zahl als Repräsentant eines Eintrags eines Elements von $\mathbf{Z}_p$.

Ein Element von $\mathbf{Z}_p$ ist somit gegeben durch eine Folge

$$a \;=\; (\cdots,\; a_{[3]} + p^3\mathbf{Z},\; a_{[2]} + p^2\mathbf{Z},\; a_{[1]} + p^1\mathbf{Z})$$

mit

$$\cdots \;\equiv_{p^3}\; a_{[3]} \;\equiv_{p^2}\; a_{[2]} \;\equiv_{p^1}\; a_{[1]} \;.$$

Wir schreiben auch kurz $a = (a_{[i]})_i := (a_{[i]} + p^i\mathbf{Z})_{i\geqslant 1} \in \mathbf{Z}_p$.

Durch eintragsweise Addition und Multiplikation wird $\prod_{i\geqslant 1} \mathbf{Z}/p^i$ zu einem Ring. Hierin ist $\mathbf{Z}_p$ ein Teilring, da für $(a_{[i]})_i$, $(b_{[i]})_i \in \mathbf{Z}_p$ sich wegen

$$a_{[i+1]} - b_{[i+1]} \;\equiv_{p^i}\; a_{[i]} - b_{[i]}$$

für $i \geqslant 1$ auch $(a_{[i]})_i - (b_{[i]})_i = (a_{[i]} - b_{[i]})_i \in \mathbf{Z}_p$ ergibt, da sich wegen

$$a_{[i+1]} \cdot b_{[i+1]} \equiv_{p^i} a_{[i]} \cdot b_{[i]}$$

für $i \geqslant 1$ auch $(a_{[i]})_i \cdot (b_{[i]})_i = (a_{[i]} \cdot b_{[i]})_i \in \mathbf{Z}_p$ ergibt, und da schließlich auch $1 = (1)_i \in \mathbf{Z}_p$ ist.

Dementsprechend heißt $\mathbf{Z}_p$ auch der *Ring der p-adischen Zahlen.*

Wir haben einen Ringmorphismus

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{Z}_p \\ z & \longmapsto & (z)_i \ . \end{array}$$

Dieser ist injektiv, da $(z)_i = 0$ bedeutet, daß $z \equiv_{p^i} 0$ für alle $i \geqslant 1$, d.h. daß $z = 0$. Wir fassen ihn als Einbettung eines Teilrings auf und schreiben $\mathbf{Z} \subseteq \mathbf{Z}_p$.

Insbesondere ist $\operatorname{char} \mathbf{Z}_p = 0$.

Für $k \geqslant 1$ gibt es einen surjektiven Ringmorphismus

$$\begin{array}{ccc} \mathbf{Z}_p & \xrightarrow{\rho_k} & \mathbf{Z}/p^k \\ (a_{[i]})_i & \longmapsto & a_{[k]} + p^k\mathbf{Z} \ . \end{array}$$

Es ist $\mathbf{Z}_p$ nullteilerfrei. *Angenommen,* nicht. Dann gibt es $(a_{[i]})_i$, $(b_{[i]})_i \in \mathbf{Z}_p \smallsetminus \{0\}$ mit $(a_{[i]}b_{[i]})_i = 0$, i.e. mit $a_{[i]}b_{[i]} \equiv_{p^i} 0$ für $i \geqslant 1$. Nun gibt es k, $\ell \geqslant 1$ mit $a_{[k]} \not\equiv_{p^k} 0$ und $b_{[\ell]} \not\equiv_{p^\ell} 0$. Es folgt $a_{[k+\ell]} \not\equiv_{p^k} 0$ und $b_{[k+\ell]} \not\equiv_{p^\ell} 0$. Somit ist $0 \equiv_{p^{k+\ell}} a_{[k+\ell]}b_{[k+\ell]} \not\equiv_{p^{k+\ell}} 0$, und wir haben einen *Widerspruch.*

Die eindeutige *p-adische Zifferndarstellung* eines Elements $a = (a_{[i]})_i \in \mathbf{Z}_p$ ist gegeben durch

$$a \ =: \ [\ldots z_4 z_3 z_2 z_1]_p \ ,$$

wobei $0 \leqslant z_i \leqslant p-1$ und $a_{[i]} \equiv_{p^i} \sum_{j=1}^{i} z_j \, p^{j-1}$ für $i \geqslant 1$.

Eine solche Zifferndarstellung breche ab, sobald nach links nur noch Nullen folgen. Diesenfalls liegt ein Element von $\mathbf{Z}_{\geqslant 0} \subseteq \mathbf{Z}_p$ vor.

Dahingegen ist

$$-1 \ = \ [\ldots (p-1)(p-1)(p-1)]_p \ ,$$

und allgemeiner

$$-[\ldots z_4 z_3 z_2 z_1]_p \ = \ [\ldots (p-1-z_4)(p-1-z_3)(p-1-z_2)(p-z_1)]_p$$

Ähnlich wie in $\mathbf{R}$ kann auch in $\mathbf{Z}_p$ bei praktischen Rechnungen im allgemeinen nur bis zu einer gewissen Genauigkeit gerechnet werden.

Beispiel.

In $\mathbf{Z}_5$ ist 2 eine Einheit, und es ergibt sich

$$1/2 \ = \ [\ldots 2223]_5$$

In $\mathbf{Z}_{11}$ ist 4 eine Einheit, und es ergibt sich

$$1/4 \;=\; [\ldots 28283]_{11}$$

Mit einer gewissen Genauigkeit wird dies auch von Magma geliefert (Reihenfolge invertiert).

```
Z := Integers();
precision := 20;
R := pAdicRing(11,precision); // auf 20 Stellen genau
Intseq(Z!(R!(1/4)) mod 11^precision,11);
```

Sei $z \in \mathbf{Z}_{\geqslant 1} \smallsetminus p\mathbf{Z}$ gegeben. Sei $k \geqslant 1$ minimal so, daß z ein Teiler von $p^k - 1$ ist. In anderen Worten, es ist k die Ordnung von $p + z\mathbf{Z}$ in $(\mathbf{Z}/z)^*$. Schreibe $p^k - 1 = zw$ mit $w \in \mathbf{Z}$, wobei natürlich $1 \leqslant w \leqslant p^k - 1$. Schreibe $w = \sum_{j=1}^{k} w_j\, p^{j-1}$ mit $w_j \in [0, p-1]$. Es ist

$$\frac{1}{1-p^k} \;=\; [\ldots 01 \underbrace{0\ldots 0}_{k-1} 1 \underbrace{0\ldots 0}_{k-1} 1]_p\,,$$

da man $(1-p^k)[\ldots 010\ldots 010\ldots 01]_p = 1$ berechnen kann. Also wird

$$-\frac{1}{z} \;=\; -\frac{w}{wz} \;=\; w\,\frac{1}{1-p^k} \;=\; w[\ldots 010\ldots 010\ldots 01]_p \;=\; [\ldots w_k \ldots w_1 w_k \ldots w_1 w_k \ldots w_1]_p$$

periodisch. Also hat $1/z$ eine ab der zweiten Stelle periodische Zifferndarstellung in $\mathbf{Z}_p$.

5 Newton-Hensel-Verfahren

Sei p prim. Sei $f(X) \in \mathbf{Z}[X]$.

Das Invertieren in $\mathbf{Z}_p$ eines Elements $z \in \mathbf{Z} \smallsetminus p\mathbf{Z}$ läuft auf die Bestimmung der Nullstelle in $\mathbf{Z}_p$ des Polynoms $zX - 1$ hinaus. Dies können wir auf beliebige Polynome in $\mathbf{Z}[X]$ verallgemeinern ([2]).

Der Zusammenhang mit unserer Fragestellung aus §3 ist folgender. Eine Nullstelle in $\mathbf{Z}_p$ von $f(X) \in \mathbf{Z}[X]$ ist eine Folge $a = (a_{[i]})_i$, wobei $a_{[i]}$ eine Nullstelle von $f(X)$ in $\mathbf{Z}/p^i$ und $a_{[i+1]} \equiv_{p^i} a_{[i]}$ ist für $i \geqslant 1$.

5.1 Taylor

Definition. Für $z \in \mathbf{Z} \smallsetminus \{0\}$ schreiben wir $z =: p^{\mathrm{v}_p(z)}\tilde{z}$ mit $\tilde{z} \in \mathbf{Z} \smallsetminus p\mathbf{Z}$ (engl. valuation, dt. Bewertung). Ferner sei $\mathrm{v}_p(0) := +\infty$.

[2] Eine Erweiterung auf Polynome in $\mathbf{Z}_p[X]$ ist ebenfalls möglich.

Ist $f(X) = \sum_{i \geqslant 0} z_i X^i \in \mathbf{Z}[X]$ ein gegebenes Polynom, so setzen wir seine (formale) Ableitung zu $f'(X) := \sum_{i \geqslant 1} i z_i X^{i-1}$.

Es gilt die Produktregel

$$(u(X)v(X))' \;=\; u'(X)v(X) + u(X)v'(X)$$

für $u(X)$, $v(X) \in \mathbf{Z}[X]$. Denn da beide Seiten $\mathbf{Z}$-bilinear in u und v sind, ist o.E. $u(X) = X^a$ und $v(X) = X^b$ für gewisse a, $b \geqslant 0$. Falls $a = 0$, dann steht auf beiden Seiten $(X^b)'$. Falls $b = 0$, dann steht auf beiden Seiten $(X^a)'$. Falls $a \geqslant 1$ und $b \geqslant 1$, dann steht links $(X^{a+b})' = (a+b)X^{a+b-1}$ und rechts $aX^{a-1}X^b + X^a bX^{b-1}$, was dasselbe gibt.

Sei $x_0 \in \mathbf{Z}$. Polynomdivision von $f(X) - f(x_0)$ durch $X - x_0$ zeigt, daß

$$f(X) \;=\; f(x_0) + (X - x_0)h(X)$$

für ein $h(X) \in \mathbf{Z}[X]$.

Wenden wir diese Tatsache nun auch noch auf $h(X)$ an, so erhalten wir

$$f(X) \;=\; f(x_0) + (X - x_0)h(x_0) + (X - x_0)^2 w(X)$$

für ein $w(X) \in \mathbf{Z}[X]$. Ableiten gibt

$$f'(X) \;=\; h(x_0) + 2(X - x_0)w(X) + (X - x_0)^2 w'(X)\ .$$

Einsetzen von x_0 liefert dann $h(x_0) = f'(x_0)$. Insgesamt erhalten wir die Taylorsche Formel in erster Näherung,

$$(*) \qquad f(X) \;=\; f(x_0) + (X - x_0)f'(x_0) + \mathrm{O}((X - x_0)^2)\ ,$$

wobei wir mit dem Landauschen $\mathrm{O}((X - x_0)^2)$-Symbol ein nicht näher interessantes Vielfaches von $(X - x_0)^2$ bezeichnen.

5.2 Existenzfragen

Lemma 1. *Sei weiterhin $f(X) \in \mathbf{Z}[X]$ gegeben.*

Sei $x_0 \in \mathbf{Z}$ mit $\mathrm{v}_p(f(x_0)) > 2\,\mathrm{v}_p(f'(x_0))$ gegeben. Schreibe $d := \mathrm{v}_p(f(x_0)) - \mathrm{v}_p(f'(x_0)) > 0$.

Wähle ein $m \in \mathbf{Z}$ mit $mf'(x_0) \equiv_{p^{2d}} f(x_0)$. Beachte, daß $\mathrm{v}_p(m) = d$, aber $\mathrm{v}_p(f'(x_0)) < d$.

Setze $x_1 := x_0 - m$.

Es ist $\mathrm{v}_p(f(x_1)) \geqslant 2d > \mathrm{v}_p(f(x_0))$.

Es ist $\mathrm{v}_p(f'(x_1)) = \mathrm{v}_p(f'(x_0))$. Mehr noch, es ist $\mathrm{v}_p(f'(x_0 + sp^d)) = \mathrm{v}_p(f'(x_0))$ für alle $s \in \mathbf{Z}$.

Insbesondere ist

$$\mathrm{v}_p(f(x_1)) \;>\; 2\,\mathrm{v}_p(f'(x_1))$$

und

$$\mathrm{v}_p(f(x_1)) - \mathrm{v}_p(f'(x_1)) \;>\; \mathrm{v}_p(f(x_0)) - \mathrm{v}_p(f'(x_0)) \;=\; d\,.$$

Lemma 1 heißt auch das *Newton-Hensel-Verfahren.* Cf. [**4,** II.§2.2].

Beweis.

Zum einen wird

$$\begin{aligned} f(x_1) &= f(x_0 - m) \\ &\overset{(*)}{=} \underbrace{f(x_0) - mf'(x_0)}_{\equiv_{p^{2d}}\, 0} + \mathrm{O}(\underbrace{m^2}_{\equiv_{p^{2d}}\, 0}) \\ &\equiv_{p^{2d}} 0\,. \end{aligned}$$

Ferner ist $2d = \mathrm{v}_p(f(x_0)) + (\mathrm{v}_p(f(x_0)) - 2\,\mathrm{v}_p(f'(x_0))) > \mathrm{v}_p(f(x_0))$.

Sei schließlich $s \in \mathbf{Z}$ gegeben. Es wird

$$f'(x_0 + sp^d) \overset{(*)}{=} \underbrace{f'(x_0)}_{\not\equiv_{p^d}\, 0} - \underbrace{sp^d f''(x_0)}_{\equiv_{p^d}\, 0} + \mathrm{O}(p^{2d})\,,$$

und also $\mathrm{v}_p(f'(x_0 + sp^d)) = \mathrm{v}_p(f'(x_0))$. □

Korollar 2. *Sei weiterhin $f(X) \in \mathbf{Z}[X]$ gegeben.*

Sei $x_0 \in \mathbf{Z}$ mit $\mathrm{v}_p(f(x_0)) > 2\,\mathrm{v}_p(f'(x_0))$ gegeben. Schreibe $d := \mathrm{v}_p(f(x_0)) - \mathrm{v}_p(f'(x_0)) > 0$.

Dann gibt es eine Folge $(x_\ell)_{\ell \geqslant 0}$ ganzer Zahlen mit

$$x_{\ell+1} \;\equiv_{p^{d+\ell}}\; x_\ell$$

und

$$\mathrm{v}_p(f(x_\ell)) \;\geqslant\; \mathrm{v}_p(f(x_0)) + \ell$$

und

$$\mathrm{v}_p(f'(x_\ell)) \;=\; \mathrm{v}_p((f'(x_0))$$

für $\ell \geqslant 0$.

Setzen wir $y = (y_{[\ell]})_{\ell \geqslant 1} := (x_\ell)_{\ell \geqslant 1} \in \mathbf{Z}_p$, so wird also $f(y) = 0$ und $\rho_d(y) = \rho_d(x_0)$.

Beweis. Die Konstruktion der Folge der x_ℓ erfolge iterativ mit Lemma 1. □

Beispiel. Sei $z \in \mathbf{Z} \smallsetminus p\mathbf{Z}$. Sei $g(X) := zX - 1$. Es ist $g'(X) = z$. Wähle $x_0 \in \mathbf{Z}$ mit $zx_0 \equiv_p 1$. Dann ist $\mathrm{v}_p(g(x_0)) > 0$ und $\mathrm{v}_p(g'(x_0)) = 0$. Also gibt es ein $x \in \mathbf{Z}_p$ mit $g(x) = 0$, i.e. mit $zx = 1$. In anderen Worten, in $\mathbf{Z}_p$ können wir $1/z$ bilden. Cf. §4.

Lemma 3. *Sei weiterhin $f(X) \in \mathbf{Z}[X]$ gegeben. Sei $x_0 \in \mathbf{Z}$ gegeben.*

Schreibe $a := \mathrm{v}_p(f(x_0))$. Sei $\ell \geqslant 1$ so, daß $f'(x_0) \equiv_{p^\ell} 0$.

Sei $k \in \mathbf{Z}$ so, daß $\frac{a}{2} < k \leqslant a$ und $k > a - \ell$.

Dann gibt es kein $x_1 \in \mathbf{Z}$ *mit* $f(x_1) \equiv_{p^{a+1}} 0$ *und* $x_1 \equiv_{p^k} x_0$.

Insbesondere gibt es kein $y \in \mathbf{Z}_p$ *mit* $f(y) = 0$ *und* $\rho_k(y) = \rho_k(x_0)$.

Ist $f'(x_0) \equiv_p 0$, dann läßt sich also x_0 nicht zu einer Nullstelle modulo $p^{\mathrm{v}_p(f(x_0))+1}$ heben.

Beweis. Annahme, es gibt ein $x_1 \in \mathbf{Z}$ mit $f(x_1) \equiv_{p^{a+1}} 0$ und $x_1 \equiv_{p^k} x_0$. Dann ist

$$0 \not\equiv_{p^{a+1}} -f(x_0) \equiv_{p^{a+1}} f(x_1) - f(x_0) \overset{(*)}{=} \underbrace{f'(x_0)}_{\equiv_{p^\ell} 0}\underbrace{(x_1 - x_0)}_{\equiv_{p^k} 0} + \mathrm{O}(\underbrace{(x_1 - x_0)^2}_{\equiv_{p^{2k}} 0}) \equiv_{p^{a+1}} 0 ,$$

und das ist ein *Widerspruch.*

Gäbe es ein $y = (y_{[i]})_i \in \mathbf{Z}_p$ mit $f(y) = 0$ und $\rho_k(y) = \rho_k(x_0)$, so wäre $f(y_{[a+1]}) \equiv_{p^{a+1}} 0$ und $y_{[a+1]} \equiv_{p^k} y_{[k]} \equiv_{p^k} x_0$, was im *Widerspruch* zum eben Gezeigten steht. □

Definition. Sei $x_0 \in \mathbf{Z}$. Sei weiterhin $f(X) \in \mathbf{Z}[X]$.

Schreibe $a := \mathrm{v}_p(f(x_0))$. Sei $a \geqslant 1$ vorausgesetzt.

Schreibe $a' := \mathrm{v}_p(f'(x_0))$. Sei $a' < +\infty$ vorausgesetzt, d.h. $f'(x_0) \neq 0$.

Wir sagen, x_0 ist eine *henselbare modulare Nullstelle* von $f(X)$, falls $a > 2a'$.

Sei $k > a'$. Wir sagen, x_0 ist eine *k-direkt henselbare modulare Nullstelle* von $f(X)$, falls $a \geqslant k + a'$.

Wegen $k > a'$ ist eine k-direkt henselbare modulare Nullstelle insbesondere henselbar.

Ist umgekehrt x_0 eine henselbare modulare Nullstelle, so ist x_0 auch k-direkt henselbar für $a' < k \leqslant a - a'$. Henselbare modulare Nullstellen sind also immer k-direkt henselbar für geeignete k.

Ist x_0 eine k-direkt henselbare modulare Nullstelle, so ist x_0 eine Nullstelle modulo p^k, die wir nach Lemma 1 zu einer Nullstelle x_1 modulo p^{k+1} heben können; hierbei ist $\mathrm{v}_p(f'(x_1)) = \mathrm{v}_p(f'(x_0))$. Dieses x_1 ist $(k+1)$-direkt henselbar, denn zum einen folgt aus $x_1 \equiv_{p^{a-a'}} x_0$ mit $a - a' \geqslant k$, daß auch $x_1 \equiv_{p^k} x_0$, zum anderen ist $\mathrm{v}_p(f(x_1)) - \mathrm{v}_p(f'(x_1))$ größer als $\mathrm{v}_p(f(x_0)) - \mathrm{v}_p(f'(x_0))$, und also größer als k.

Ist x_0 eine k-direkt henselbare modulare Nullstelle für ein $k > a'$, so ist auch $x_0 + sp^k$ eine k-direkt henselbare modulare Nullstelle für alle $s \in \mathbf{Z}$. Denn zum einen ist

$$f(x_0 + sp^k) \overset{(*)}{=} f(x_0) + sp^k f'(x_0) + \mathrm{O}(p^{2k}) \equiv_{p^{k+a'}} 0 ,$$

zum anderen ist

$$f'(x_0 + sp^k) \overset{(*)}{=} f'(x_0) + sp^k f''(x_0) + \mathrm{O}(p^{2k}) \equiv_{p^{a'+1}} f'(x_0) ,$$

und also $\mathrm{v}_p(f'(x_0 + sp^k)) = a'$.

Bemerkung. Sei weiterhin $f(X) \in \mathbf{Z}[X]$. Sei ein $y = (y_{[i]})_i \in \mathbf{Z}_p$ mit $f(y) = 0$ gegeben. In anderen Worten, sei $f(y_{[i]}) \equiv_{p^i} 0$ für alle $i \geqslant 1$.

Im Hebungsbaum zeigt sich ein solches y als unendlicher Kantenzug.

Sei $a' := \mathrm{v}_p(f'(y))$, wobei v_p in kanonischer Weise von $\mathbf{Z}$ nach $\mathbf{Z}_p$ ausgedehnt wurde. Sei $f'(y) \neq 0$, i.e. $a' \neq +\infty$ vorausgesetzt. In anderen Worten, es gebe ein $j \geqslant 1$ mit $f'(y_{[j]}) \not\equiv_{p^j} 0$, für welches wir $a' := \mathrm{v}_p(f'(y_{[j]}))$ setzen.

Dann ist $\mathrm{v}_p(f'(y_{[i]})) = a'$ für $i > a'$. Da $\mathrm{v}_p(f(y_{[i]})) \geqslant i$ für alle $i \geqslant 1$ ist, folgt, daß $y_{[i]}$ eine henselbare modulare Nullstelle ist für $i > 2a'$.

Kurz, gibt es ein $y \in \mathbf{Z}_p$ mit $f(y) = 0$, aber $f'(y) \neq 0$, dann hat $f(X)$ auch eine henselbare modulare Nullstelle. Cf. auch Nicht-Beispiel am Ende von §6.

5.3 Eindeutigkeitsfragen

Lemma 4. *Sei weiterhin $f(X) \in \mathbf{Z}[X]$ gegeben. Sei $k \geqslant 1$. Sei $x_0 \in \mathbf{Z}$ so, daß $f(x_0) \equiv_{p^k} 0$. Sei $1 \leqslant \ell \leqslant k$ so, daß $f'(x_0) \equiv_{p^\ell} 0$.*

Ist $x_1 \in \mathbf{Z}$ mit $f(x_1) \equiv_{p^{k+\ell}} 0$ und $x_1 \equiv_{p^k} x_0$ gegeben, dann ist auch $f(x_1 + sp^k) \equiv_{p^{k+\ell}} 0$ für alle $s \in \mathbf{Z}$.

Beweis. Wir rechnen

$$f(x_1 + sp^k) \overset{(*)}{=} f(x_1) + sp^k f'(x_1) + \mathrm{O}(p^{2k}) \equiv_{p^{k+\ell}} sp^k f'(x_1) \equiv_{p^{k+\ell}} sp^k f'(x_0) \equiv_{p^{k+\ell}} 0 \,.$$

□

Lemma 5. *Sei weiterhin $f(X) \in \mathbf{Z}[X]$ gegeben. Sei $k \geqslant 1$. Sei $x_0 \in \mathbf{Z}$ so, daß $f(x_0) \equiv_{p^k} 0$. Sei $1 \leqslant \ell \leqslant k$ so, daß $f'(x_0) \not\equiv_{p^\ell} 0$.*

Ist $x_1 \in \mathbf{Z}$ mit $f(x_1) \equiv_{p^{k+\ell}} 0$ und $x_1 \equiv_{p^k} x_0$ gegeben, dann ist $f(x_1 + sp^k) \not\equiv_{p^{k+\ell}} 0$ für alle $s \in \mathbf{Z} \smallsetminus p\mathbf{Z}$.

Beweis. Wir rechnen

$$f(x_1 + sp^k) \overset{(*)}{=} f(x_1) + sp^k f'(x_1) + \mathrm{O}(p^{2k}) \equiv_{p^{k+\ell}} sp^k f'(x_1) \equiv_{p^{k+\ell}} sp^k f'(x_0) \not\equiv_{p^{k+\ell}} 0 \,.$$

□

Korollar 6. *Sei weiterhin $f(X) \in \mathbf{Z}[X]$ gegeben. Seien $x_0 \in \mathbf{Z}$ und $k \geqslant 1$ so gegeben, daß $f(x_0) \equiv_{p^k} 0$. Es ist*

$$|\{t \in [0, p^{k+1} - 1] \,:\, f(t) \equiv_{p^{k+1}} 0,\ t \equiv_{p^k} x_0\}| \in \{0, 1, p\} \,.$$

Eine Nullstelle modulo p^k kann also auf keine, eine oder p Weisen zu einer Nullstelle modulo p^{k+1} gehoben werden.

Beweis. Gebe es ein $x_1 \in [0, p^{k+1} - 1]$ mit $f(x_1) \equiv_{p^{k+1}} 0$ und $x_1 \equiv_{p^k} x_0$.

Fall $f'(x_0) \equiv_p 0$. Nach Lemma 4, angewandt mit $\ell := 1$, ist $f(x_1 + sp^k) \equiv_{p^{k+1}} 0$ für alle $s \in \mathbf{Z}$. Somit ist

$$\{t \in [0, p^{k+1} - 1] \ : \ f(t) \equiv_{p^{k+1}} 0, \ t \equiv_{p^k} x_0\} \ = \ \{t \in [0, p^{k+1} - 1] \ : \ t \equiv_{p^k} x_0\}$$

und besteht aus p Elementen.

Fall $f'(x_0) \not\equiv_p 0$. Nach Lemma 5, angewandt mit $\ell := 1$, ist

$$\{t \in [0, p^{k+1} - 1] \ : \ f(t) \equiv_{p^{k+1}} 0, \ t \equiv_{p^k} x_0\} \ = \ \{x_1\}$$

und besteht aus einem Element. □

Lemma 7. *Sei weiterhin* $f(X) \in \mathbf{Z}[X]$ *gegeben. Sei* $x_0 \in \mathbf{Z}$. *Sei* $a' := \mathrm{v}_p(f'(x_0))$. *Sei* $k > a'$. *Sei* x_0 *eine* k*-direkt henselbare modulare Nullstelle von* $f(X)$.

Dann gibt es genau eine $(k+1)$*-direkt henselbare modulare Nullstelle* $x_1 \in \mathbf{Z}$ *von* $f(X)$ *mit* $x_1 \in [0, p^{k+1} - 1]$ *und* $x_1 \equiv_{p^k} x_0$. *Es ist* $\mathrm{v}_p(f'(x_1)) = a'$.

Ferner ist $\mathrm{v}_p(f(x_1 + sp^k)) \leqslant k + a'$ *für alle* $s \in \mathbf{Z} \setminus p\mathbf{Z}$.

Beweis. Die Existenz einer $(k+1)$-direkt henselbaren modularen Nullstelle $x_1 \in \mathbf{Z}$ von $f(X)$ mit $x_1 \in [0, p^{k+1} - 1]$ und $x_1 \equiv_{p^k} x_0$ wurde schon in §5.2 angemerkt, unmittelbar bei der Definition.

Sei $s \in \mathbf{Z} \setminus p\mathbf{Z}$. Wir haben zu zeigen, daß $f(x_1 + sp^k)$ keine $(k+1)$-direkt henselbare modulare Nullstelle von $f(X)$ ist. In §5.2 wurde schon bemerkt, daß $\mathrm{v}_p(f'(x_1)) = a'$. Es wird

$$f(x_1 + sp^k) \ \overset{(*)}{=} \ f(x_1) + sp^k f'(x_1) + \mathrm{O}(p^{2k}) \ \equiv_{p^{k+a'+1}} \ sp^k f'(x_1) \ \not\equiv_{p^{k+a'+1}} \ 0 \ .$$

□

6 Henselbare Nullstellen in den Hebungsbäumen

Wir setzen die Beispiele aus §2 fort, indem wir jeweils die Aussagen von §5 zur Anwendung bringen. Hierbei seien die Nullstellen modulo p durch eine direkte Suche bekannt; davon ausgehend versuchen wir, mit theoretischen Mitteln den Hebungsbaum im endlichen Fall möglichst ohne weitere Suche zu rekonstruieren, sowie im unendlichen Fall überhaupt erst einmal komplett zu beschreiben.

Sei p prim.

Beispiel. Betrachte $u_1(X) = X^2 + X + 1$ bei $p = 3$. Der Hebungsbaum hat nur den Eintrag 1 in Ebene 1.

1

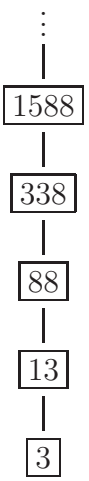
Es ist $\mathrm{v}_3(u_1(1)) = 1$ und $\mathrm{v}_3(u_1'(1)) = 1$. Insbesondere ist 1 keine henselbare modulare Nullstelle, da $\mathrm{v}_3(u_1(1)) = 1 \leqslant 2 = 2\,\mathrm{v}_3(u_1'(1))$.

```
Z := Integers();
Q := Rationals();
P<X> := PolynomialRing(Q);
p := 3;
u := X^2 + X + 1;
uu := Derivative(u);
print Valuation(Z!Evaluate(u,1),p), Valuation(Z!Evaluate(uu,1),p);
```

In der Bezeichnung von Lemma 3 haben wir $f(X) = u_1(X)$, $x_0 = 1$, $a = \mathrm{v}_3(u_1(1)) = 1$, $\mathrm{v}_p(f'(1)) = \mathrm{v}_3(u_1'(1)) = 1$, und können $k := 1$ und $\ell := 1$ setzen. Also gibt es kein $x_1 \in \mathbf{Z}$ mit $u_1(x_1) \equiv_9 0$ und $x_1 \equiv_3 1$. In anderen Worten, wir können die Nullstelle 1 modulo 3 nicht zu einer Nullstelle modulo 9 heben.

Beispiel. Betrachte $u_2(X) = X^4+X+1$ bei $p = 5$. Wir erhalten folgenden Hebungsbaum, in welchem wir in der k-ten Ebene die k-direkt henselbaren modularen Nullstellen markiert haben, viz. alle.

Es ist $u_2'(3) \not\equiv_5 0$.

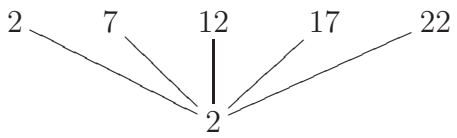



```
Z := Integers();
Q := Rationals();
P<X> := PolynomialRing(Q);
p := 5;
u := X^4 + X + 1;
uu := Derivative(u);
for x in [3,13,88,338,1588] do
 a := Valuation(Z!Evaluate(u,x),p); aa := Valuation(Z!Evaluate(uu,x),p);
 print x, a, aa, a - 2*aa;
end for;
```

Korollar 2 findet Anwendung.

Lemma 5 jeweils mit $\ell = 1$ angewandt liefert die Eindeutigkeit der Hebungen. Insbesondere haben wir nun sichergestellt, daß der Baum sich wie erwartet als einzelner Zweig fortsetzt.

Beispiel. Betrachte $u_3(X) = X^4 + 3X + 3$ bei $p = 5$. Wir erhalten folgenden Hebungsbaum, in welchem kein Eintrag eine henselbare modulare Nullstelle ist. Es ist $\mathrm{v}_5(u_3(2)) = 2$ und $\mathrm{v}_5(u_3'(2)) = 1$.

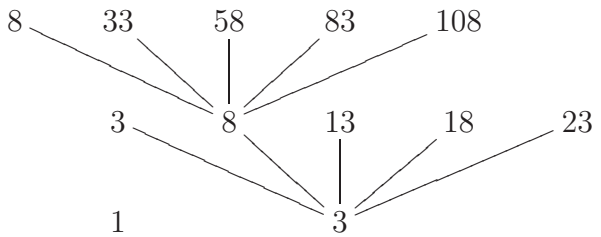


Die Nullstelle 2 modulo 5 hebt wegen $\mathrm{v}_5(u_3(2)) = 2$ natürlich zur Nullstelle 2 modulo 25. Gemäß Lemma 4, angewandt mit $k = 1$ und $\ell = 1$, sind also auch 7, 12, 17 und 22 Nullstellen modulo 25.

Wenden wir Lemma 3 auf $x_0 = 2$ an, so wird $a := \mathrm{v}_5(u_3(2)) = 2$, so daß wir $\ell := 1$ und $k := 2$ setzen können. Wir erhalten so die Aussage, daß es kein $x_1 \in \mathbf{Z}$ gibt mit $u_3(x_1) \equiv_{125} 0$ und $x_1 \equiv_{25} 2$. Wir können also die Nullstelle 2 modulo 25 nicht zu einer Nullstelle modulo 125 heben.

Genauso die Nullstellen 7, 12, 17 und 22 modulo 25. Berichtenswert ist hierbei noch, daß $\mathrm{v}_5(u_3'(7)) = 3$ und dort natürlich trotzdem Lemma 3 mit $\ell := 1$ verwandt werden kann.

Beispiel. Betrachte $u_4(X) = X^4 - 3X^3 - 3X^2 + X - 1$ bei $p = 5$. Wir erhalten folgenden Hebungsbaum, in welchem kein Eintrag eine henselbare modulare Nullstelle ist.



Zur modularen Nullstelle 1. In der Bezeichnung von Lemma 3 haben wir $f(X) = u_4(X)$, $x_0 = 1$, $a = 1$, $\mathrm{v}_p(f'(1)) = \mathrm{v}_p(u_4'(1)) = 1$, und können $k := 1$ und $\ell := 1$ setzen. Also gibt es kein $x_1 \in \mathbf{Z}$ mit $u_4(x_1) \equiv_{25} 0$ und $x_1 \equiv_5 1$. In anderen Worten, wir können die Nullstelle 1 modulo 5 nicht zu einer Nullstelle modulo 25 heben.

Zur modularen Nullstelle 3. Es ist $\mathrm{v}_5(u_4(3)) = 2$ und $\mathrm{v}_5(u_4'(3)) = 1$.

Die Nullstelle 3 modulo 5 hebt wegen $\mathrm{v}_5(u_4(3)) = 2$ natürlich zur Nullstelle 3 modulo 25. Gemäß Lemma 4, angewandt mit $k = 1$ und $\ell = 1$, sind also auch 3, 8, 13, 18 und 23 Nullstellen modulo 25.

Wenden wir Lemma 3 auf $x_0 = 3$ an, so wird $a := \mathrm{v}_5(u_4(2)) = 2$, so daß wir $\ell := 1$ und $k := 2$ setzen können. Wir erhalten so die Aussage, daß es kein $x_1 \in \mathbf{Z}$ gibt mit $u_3(x_1) \equiv_{125} 0$ und $x_1 \equiv_{25} 3$. Wir können also die Nullstelle 3 modulo 25 nicht zu einer

Nullstelle modulo 125 heben.

Genauso die Nullstellen 13, 18 und 23 modulo 25.

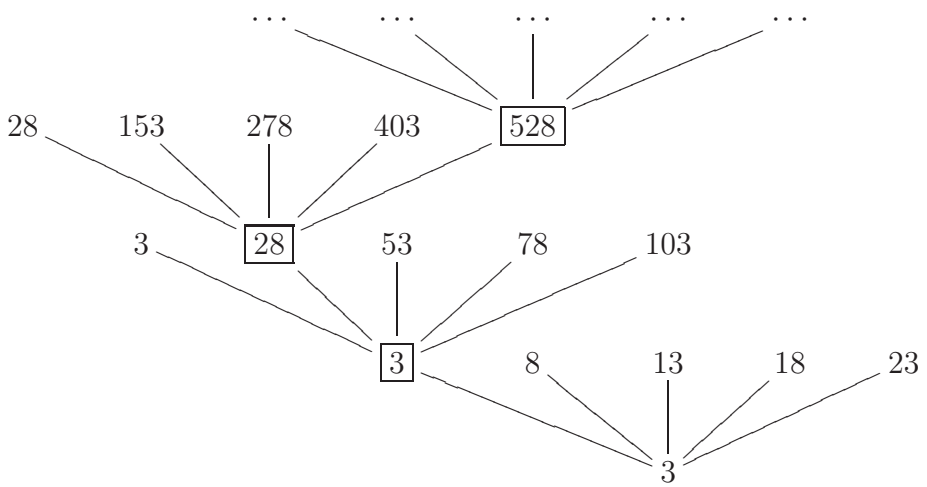
Es ist $\mathrm{v}_5(u_4(8)) = 3$ und $\mathrm{v}_5(u_4'(8)) = 2$.

Die Nullstelle 8 modulo 25 hebt wegen $\mathrm{v}_5(u_4(8)) = 3$ natürlich zur Nullstelle 8 modulo 125. Gemäß Lemma 4, angewandt mit $k = 2$ und $\ell = 1$, sind also auch 33, 58, 83 und 108 Nullstellen modulo 125.

Wenden wir Lemma 3 auf $x_0 = 8$ an, so wird $a := \mathrm{v}_5(u_4(8)) = 3$, so daß wir $\ell := 1$ und $k := 3$ setzen können. Wir erhalten so die Aussage, daß es kein $x_1 \in \mathbf{Z}$ gibt mit $u_4(x_1) \equiv_{625} 0$ und $x_1 \equiv_{125} 8$. Wir können also die Nullstelle 8 modulo 125 nicht zu einer Nullstelle modulo 625 heben.

Genauso die Nullstellen 33, 58, 83 und 108 modulo 125. Berichtenswert ist noch, daß $\mathrm{v}_5(u_2'(33)) = 4$.

Beispiel. Betrachte $u_5(X) = X^6 - 6X^3 - 6X^2 - 5X + 2$ bei $p = 5$. Wir erhalten folgenden Hebungsbaum, in welchem wir in der k-ten Ebene die k-direkt henselbaren modularen Nullstellen markiert haben.



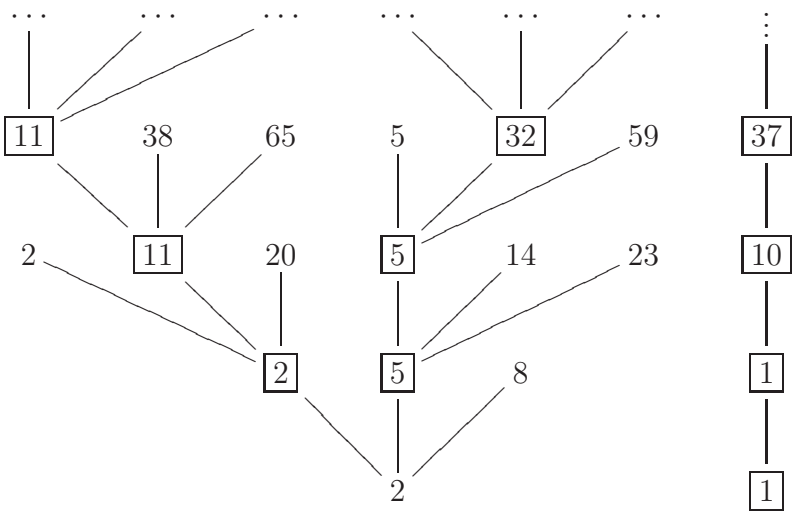
Von den dargestellten Einträgen sind 3, 28, 53, 78, 103, 153, 278, 403 und 528 henselbare modulare Nullstellen.

Es ist $\mathrm{v}_5(u_5(3)) = 3$ und $\mathrm{v}_5(u_5'(3)) = 1$.

Es ist 3 eine Nullstelle modulo 25. Dank Lemma 4 sind auch 8, 13, 18 und 23 Nullstellen modulo 25. Dank Lemma 3 lassen sich letztere nicht heben.

Da 3 eine 2-direkt henselbare modulare Nullstelle ist, ergibt sich die Gestalt (wenn auch nicht die genauen Einträge) des restlichen Baumes aus Lemma 7, Lemma 4 und Lemma 3.

Beispiel. Betrachte $u_6(X) = X^3 + X^2 - X + 17$ bei $p = 3$. Wir erhalten folgenden Hebungsbaum, in welchem wir in der k-ten Ebene die k-direkt henselbaren modularen Nullstellen markiert haben.



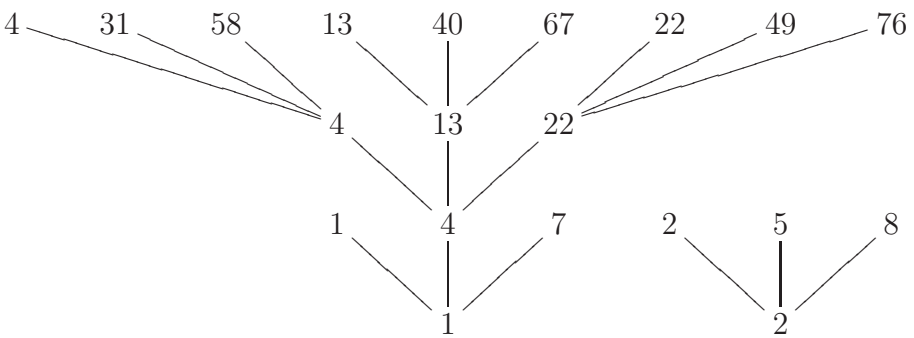
Unter den angeführten Einträgen ist nur 8 keine henselbare modulare Nullstelle.

Da 1 eine 1-direkt henselbare modulare Nullstelle ist, ergibt sich die Gestalt (wenn auch nicht die genauen Einträge) des rechten Baumteils aus Lemma 5 und Lemma 7.

Es ist 2 eine Nullstelle modulo 9. Dank Lemma 4 sind auch 5 und 8 Nullstellen modulo 9. Dank Lemma 3 läßt sich 8 nicht heben.

Da 2 und 5 zwei 2-direkt henselbare modulare Nullstellen sind, ergibt sich die Gestalt (wenn auch nicht die genauen Einträge) des restlichen Baumes aus Lemma 7, Lemma 4 und Lemma 3.

Beispiel. Betrachte $u_7(X) = X^6 - 4X^4 - 6X^3 + 5X^2 - 3X - 2$ bei $p = 3$. Wir erhalten folgenden Hebungsbaum, in welchem kein Eintrag eine henselbare modulare Nullstelle ist.

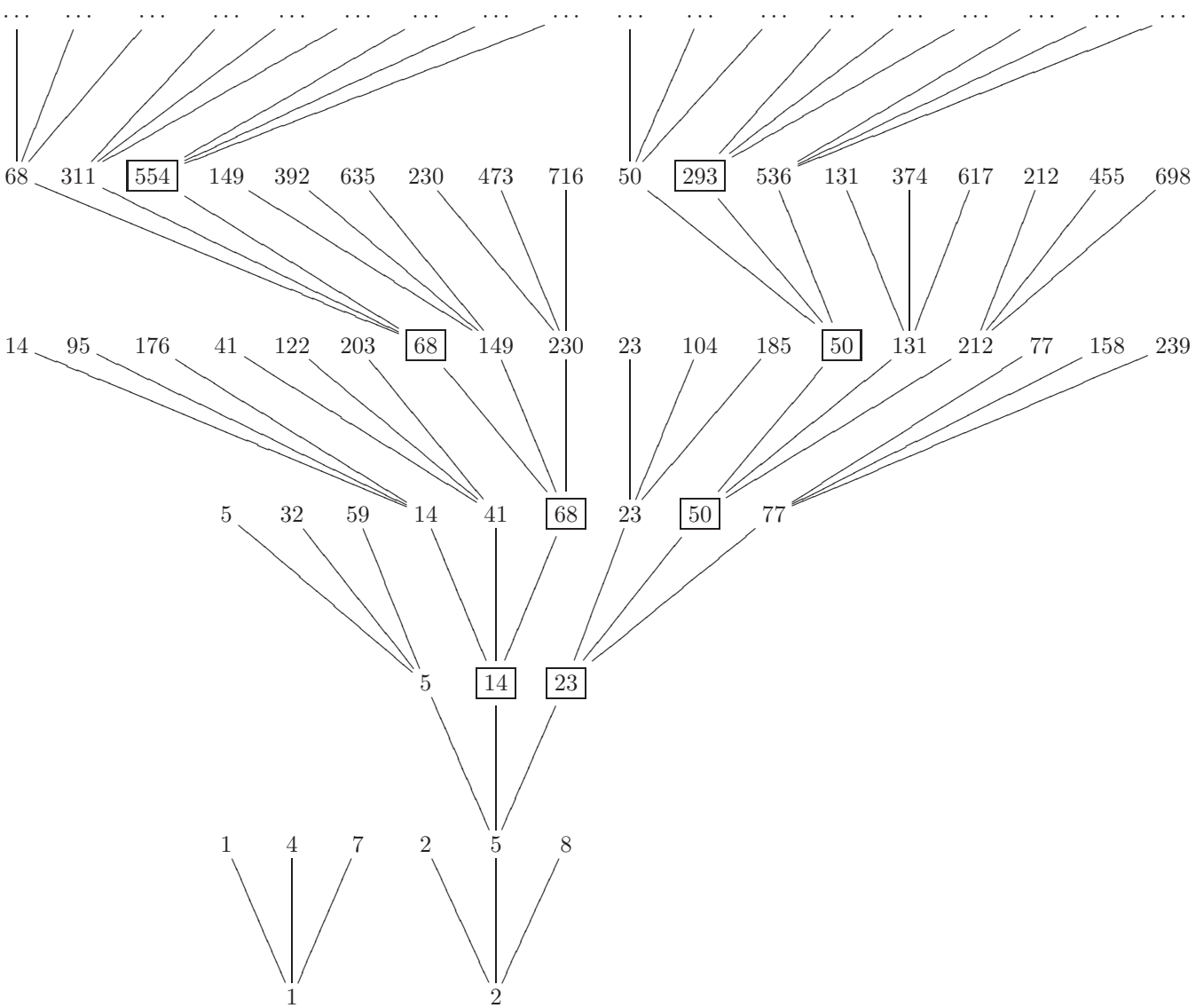


Es ist 2 eine Nullstelle modulo 9. Dank Lemma 4 sind auch 5 und 8 Nullstellen modulo 9. Dank Lemma 3 lassen sich weder 2 noch 5 noch 8 zu einer Nullstelle modulo 27 heben.

Es ist 1 eine Nullstelle modulo 9. Dank Lemma 4 sind auch 4 und 7 Nullstellen modulo 9. Dank Lemma 3 lassen sich weder 1 noch 7 zu einer Nullstelle modulo 27 heben.

Es ist 4 eine Nullstelle modulo 81. Dank Lemma 4 sind auch 4, 31, 58, 13, 40, 67, 22, 49 und 76 Nullstellen modulo 81. Dank Lemma 3 läßt sich keine von diesen zu einer Nullstelle modulo 243 heben.

Beispiel. Betrachte $u_8(X) = X^6 - X^4 - 6X^3 - 4X^2 + 6X - 5$ bei $p = 3$. Wir erhalten folgenden Hebungsbaum, in welchem wir in der k-ten Ebene die k-direkt henselbaren modularen Nullstellen markiert haben.



Unter den angeführten Einträgen sind 1, 4, 7, 2, 5, 8, 32 und 59 keine henselbaren modularen Nullstellen.

Es ist 1 eine Nullstelle modulo 9. Dank Lemma 4 sind auch 4 und 7 Nullstellen modulo 9. Dank Lemma 3 lassen sich weder 1 noch 4 noch 7 zu einer Nullstelle modulo 27 heben.

Es ist 2 eine Nullstelle modulo 9. Dank Lemma 4 sind auch 5 und 8 Nullstellen modulo 9. Dank Lemma 3 lassen sich weder 2 noch 8 zu einer Nullstelle modulo 27 heben.

Es ist 5 eine Nullstelle modulo 81. Dank Lemma 4 sind auch 14, 23, 32, 41, 50, 59, 68 und 77 Nullstellen modulo 81. Dank Lemma 3 lassen sich weder 5 noch 32 noch 59 zu einer Nullstelle modulo 243 heben.

Es sind 14 und 23 zwei 3-direkt henselbare modulare Nullstellen. Damit ergibt sich die Form (ohne Einträge) des weiteren Baums wie folgt.

Betrachten wir einmal die 14. Diese gibt nach Lemma 7 Anlaß zu genau einem unendlichen Kantenzug, welcher in Ebene $k \geqslant 3$ einen k-direkt henselbaren Eintrag hat.

Gemäß Lemma 4 hebt 14 zu insgesamt 8 nicht 5-direkt henselbaren modularen Nullstellen modulo 243 in $[0, 242]$. Bei diesen hat u_8 also Bewertung $\geqslant 5$. Nach Lemma 7 hat u_8 bei den 6 Einträgen davon, die nicht kongruent modulo 3 zur 4-direkt henselbaren Hebung 68 von 14 sind, aber Bewertung $\leqslant 5$. Diese 6 Einträge sehen wir im Baum also in der 5-ten Ebene, und zwar über 14 aus der 3-ten Ebene, nicht aber über 68 aus der 4-ten Ebene: 14, 95, 176, 41, 122 und 203. Dank Lemma 3 hebt nun keine dieser 6 Nullstellen zu einer Nullstelle modulo 729.

Genauso fahre man fort zu argumentieren mit 68 in der 4-ten Ebene, mit 68 in der 5-ten Ebene, mit 554 in der 6-ten Ebene, usf. Beachte dabei, daß nach Lemma 7 die Bewertung v_3 der Auswertung von u_8' an jeder k-direkt henselbaren Nullstelle über 14 gleich der Bewertung der Ableitung bei 14 ist, nämlich 2. Beachte ferner, daß die jeweilige Anwendung von Lemma 3 ohne weitere Rechnung vonstatten gehen kann, da man die dafür nötigen Bewertungen schon von Lemma 7 geliefert bekommt.

Analog der Kantenzug, der bei 23 in der 3-ten Ebene beginnt.

Nicht-Beispiel. Sei $u_9(X) := X^2$. Sei $p = 2$. Für die modulare Nullstelle 0 ist Henselbarkeit nicht definiert. Keine modulare Nullstelle $z \in 2\mathbf{Z} \smallsetminus \{0\}$ ist henselbar, da dort $\mathrm{v}_2(u_9(z)) - 2\,\mathrm{v}_2(u_9'(z)) = \mathrm{v}_2(z^2) - 2\,\mathrm{v}_2(2z) = 2\,\mathrm{v}_2(z) - 2(\mathrm{v}_2(z) + 1) = -2$ ist.

Wende die Aussagen aus §5 auf die selbstgefundenen Beispiele an!

Besonders interessant sind hierbei Beispiele, in denen die Theorie nicht zu einer Erklärung des Hebungsbaums ausreicht.

7 Zerlegung in irreduzible Faktoren in $\mathbf{Z}_p[X]$

Sei p prim.

Es verfügt im Gegensatz zu den Ringen $(\mathbf{Z}/p^k)[X]$ für $k \geqslant 2$ der Ring $\mathbf{Z}_p[X]$ über eine (bis auf Reihenfolge der Faktoren) eindeutige Zerlegung eines normierten Polynoms in irreduzible normierte Polynome.

Begründe diese Aussage!

Sei $f(X) \in \mathbf{Z}[X]$. Die Anzahl der unendlichen Kantenzüge im Hebungsbaum von $f(X)$ ist durch den Grad von $f(X)$ nach oben beschränkt. Denn $f(X)$ kann in $\mathbf{Z}_p$ höchstens

deg f verschiedene Nullstellen haben.

Da char $\mathbf{Q} = 0$, ist $\mathbf{Q}$ separabel. Also hat ein in $\mathbf{Z}[X]$ irreduzibles normiertes Polynom in $\mathbf{Z}_p[X]$ irreduzible Faktoren nur von Multiplizität 1, und insbesondere Nullstellen nur von Multiplizität 1.

Wir zerlegen $f(X)$ via Magma mit einer gewissen Genauigkeit in $\mathbf{Z}_p[X]$ in unseren Beispielen, i.e. mit einer gewissen Stellenzahl in $\mathbf{Z}_p$ in der p-adischen Darstellung.

Diese Genauigkeit `s` sollte, setzt man `t := Valuation(Discriminant(f),p)`, mindestens `t + (Degree(f)-1)*(t div 2) + 1` Stellen sein. Warum dies so ist, wird im fakultativen Anhang A erläutert; siehe die Anwendung dort. Wir müssen unser gegebenes Polynom mit Genauigkeit von `s` Stellen via Magma zerlegen. Es resultieren `m` Faktoren. Dann müssen wir testen, ob diese Zerlegung bei einer Rechnung auf `s - (m-1)*(t div 2)` Stellen genau weiter zerfällt. Ist dies nicht der Fall, so haben wir in der auf `s` Stellen genauen Zerlegung die irreduziblen Faktoren in $\mathbf{Z}_p[X]$ erhalten, welche wir dort aber nur auf `s - (m-1)*(t div 2)` Stellen genau sehen.

Beispiel. Betrachte $u_1(X) := X^2 + X + 1$ bei $p = 3$. Es ist die Diskriminante gleich -3, und also brauchen wir eine Genauigkeit von mindestens

$$\mathrm{v}_3(-3) + (\deg u_1 - 2)\lfloor \mathrm{v}_3(-3)/2 \rfloor + 1 \;=\; 2$$

Stellen. Bei einer Berechnung auf 2 Stellen genau bleibt $u_1(X)$ in $\mathbf{Z}_3[X]$ irreduzibel. Bei einer Berechnung auf $2 - (1-1)\cdot\lfloor \mathrm{v}_3(-3)/2 \rfloor = 2$ Stellen genau ändert sich natürlich nichts. Also ist $u_1(X)$ in $\mathbf{Z}_3[X]$ irreduzibel.

In der Tat konnten wir im Hebungsbaum in §6 auch keine Nullstelle von $u_1(X)$ in $\mathbf{Z}_3$ erkennen.

```
R := pAdicRing(3,2); // die 2 ist die Genauigkeit
P<X> := PolynomialRing(R);
u1 := P ! X^2+X+1;
Factorisation(u1);
```

Es ist hier und im folgenden auch interessant, ein wenig mit der Genauigkeit zu spielen, sie einmal etwas zu tief anzusetzen, etc.

Beispiel. Betrachte $u_2(X) := X^4 + X + 1$ bei $p = 5$. Es ist die Diskriminante gleich 229, und also brauchen wir eine Genauigkeit von mindestens

$$\mathrm{v}_5(229) + (\deg u_2 - 2)\lfloor \mathrm{v}_5(229)/2 \rfloor + 1 \;=\; 1$$

Stellen. Bei einer Berechnung auf 1 Stelle genau zerfällt $u_2(X)$ in $\mathbf{Z}_5[X]$ in ein Produkt irreduzibler Faktoren von Grad 1 und 3, und bei einer Berechnung auf

$$1 - (2-1)\cdot\lfloor \mathrm{v}_5(229)/2 \rfloor \;=\; 1$$

Stelle genau ändert sich natürlich nichts. Also haben wir $u_2(X)$ in $\mathbf{Z}_5[X]$ in irreduzible Faktoren zerlegt, und sehen diese auf 1 Stelle genau.

Den Linearfaktor haben wir als einzige Nullstelle von $u_2(X)$ in $\mathbf{Z}_5$ im Hebungsbaum in §6 gesehen.

```
R := pAdicRing(5,1);
P<X> := PolynomialRing(R);
u2 := P ! X^4+X+1;
Factorisation(u2);
```

Beispiel. Betrachte $u_3(X) = X^4+3X+3$ bei $p = 5$. Es ist die Diskriminante gleich 4725, damit $\mathrm{v}_5(4725) = 2$, und also brauchen wir eine Genauigkeit von mindestens

$$\mathrm{v}_5(4725) + (\deg u_3 - 2)\lfloor \mathrm{v}_5(4725)/2 \rfloor + 1 = 5 \; .$$

Stellen. Bei einer Berechnung auf 5 Stellen genau zerfällt $u_3(X)$ in $\mathbf{Z}_5[X]$ in ein Produkt zweier irreduzibler Faktoren vom Grad 2, und bei einer Berechnung auf

$$5 - (2-1) \cdot \lfloor \mathrm{v}_5(4725)/2 \rfloor \; = \; 4$$

Stellen genau zerfallen diese nicht weiter. Also haben wir $u_3(X)$ in $\mathbf{Z}_5[X]$ in irreduzible Faktoren zerlegt, und sehen diese in ersterer Berechnung auf 4 Stellen genau.

Im Hebungsbaum in §6 konnten wir ebenfalls keine Nullstelle von $u_3(X)$ in $\mathbf{Z}_5$ erkennen.

```
R := pAdicRing(5,5);
P<X> := PolynomialRing(R);
u3 := P ! X^4+3*X+3;
fac := Factorisation(u3);
print fac;

R := pAdicRing(5,4);
P<X> := PolynomialRing(R);
Factorisation(P!fac[1][1]);
Factorisation(P!fac[2][1]);
```

Beispiel. Betrachte $u_4(X) = X^4 - 3X^3 - 3X^2 + X - 1$ bei $p = 5$. Es ist die Diskriminante gleich -11875, damit $\mathrm{v}_5(-11875) = 4$, und also brauchen wir eine Genauigkeit von mindestens

$$\mathrm{v}_5(-11875) + (\deg u_4 - 2)\lfloor \mathrm{v}_5(-11875)/2 \rfloor + 1 = 9$$

Stellen. Bei einer Berechnung auf 9 Stellen genau zerfällt $u_4(X)$ in $\mathbf{Z}_5[X]$ in ein Produkt zweier irreduzibler Faktoren vom Grad 2, und bei einer Berechnung auf

$$9 - (2-1) \cdot \lfloor \mathrm{v}_5(-11875)/2 \rfloor \; = \; 7$$

Stellen genau zerfallen diese nicht weiter. Also haben wir $u_4(X)$ in $\mathbf{Z}_5[X]$ in irreduzible Faktoren zerlegt, und sehen diese in ersterer Berechnung auf 7 Stellen genau.

Im Hebungsbaum in §6 konnten wir ebenfalls keine Nullstelle von $u_4(X)$ in $\mathbf{Z}_5$ erkennen.

Beispiel. Betrachte $u_5(X) = X^6 - 6X^3 - 6X^2 - 5X + 2$ bei $p = 5$. Es ist die Diskriminante gleich 253056125, damit $\mathrm{v}_5(253056125) = 3$, und also brauchen wir eine Genauigkeit von mindestens

$$\mathrm{v}_5(253056125) + (\deg u_5 - 2)\lfloor \mathrm{v}_5(253056125)/2 \rfloor + 1 \;=\; 8$$

Stellen. Bei einer Berechnung auf 8 Stellen genau zerfällt $u_5(X)$ in $\mathbf{Z}_5[X]$ in ein Produkt irreduzibler Faktoren von Grad 1, 2 und 3, und bei einer Berechnung auf

$$8 - (3-1) \cdot \lfloor \mathrm{v}_5(253056125)/2 \rfloor \;=\; 6$$

Stellen genau zerfallen diese nicht weiter. Also haben wir $u_5(X)$ in $\mathbf{Z}_5[X]$ in irreduzible Faktoren zerlegt, und sehen diese in ersterer Berechnung auf 6 Stellen genau.

Den Linearfaktor haben wir als einzige Nullstelle von $u_5(X)$ in $\mathbf{Z}_5$ im Hebungsbaum in §6 gesehen.

```
R := pAdicRing(5,8);
P<X> := PolynomialRing(R);
u5 := P ! X^6-6*X^3-6*X^2-5*X+2;
fac := Factorisation(u5);
print fac;

R:=pAdicRing(5,6);
P<X>:=PolynomialRing(R);
Factorisation(P!fac[1][1]);
Factorisation(P!fac[2][1]);
Factorisation(P!fac[3][1]);
Factorisation(P ! u5); // out of interest
```

> Versucht man also, anders vorzugehen und $u_5(X)$ über `pAdicRing(5,6)` abermals in Faktoren zu zerlegen, um dann zu vergleichen, so wird man mit dem Problem konfrontiert, daß in $(\mathbf{Z}/5^6)[X]$ die Zerlegung in irreduzible Faktoren im allgemeinen nicht eindeutig ist.

Beispiel. Betrachte $u_6(X) = X^3 + X^2 - X + 17$ bei $p = 3$. Es ist die Diskriminante gleich -8172, damit $\mathrm{v}_3(-8172) = 2$, und also brauchen wir eine Genauigkeit von mindestens

$$\mathrm{v}_3(-8172) + (\deg u_6 - 2)\lfloor \mathrm{v}_3(-8172)/2 \rfloor + 1 = 4$$

Stellen. Bei einer Berechnung auf 4 Stellen genau zerfällt $u_6(X)$ in $\mathbf{Z}_3[X]$ in ein Produkt dreier Linearfaktoren, welches natürlich auch bei einer Berechnung auf

$$4 - (3-1) \cdot \lfloor \mathrm{v}_3(-8172)/2 \rfloor \;=\; 2$$

Stellen genau nicht weiter zerfällt. Also haben wir $u_6(X)$ in $\mathbf{Z}_3[X]$ in irreduzible Faktoren zerlegt, und sehen diese in ersterer Berechnung auf 2 Stellen genau.

Diese Linearfaktoren haben wir als Nullstellen von $u_6(X)$ in $\mathbf{Z}_3$ im Hebungsbaum in §6 gesehen.

Schreiben wir $u_6(X) = (X-\alpha)(X-\beta)(X-\gamma)$ in $\mathbf{Z}_3[X]$, so ist (bei geeigneter Reihenfolge) $\alpha \equiv_3 \beta \not\equiv_3 \gamma$. Dies hat zur Folge, daß für $k \geqslant 1$ aus $x_0 \equiv_{3^k} \alpha$ immer auch $x_0 \equiv_3 \beta$ folgt, und also $u_6(x_0) \equiv_{3^{k+1}} 0$ gilt. Ändern wir x_0 um ein Vielfaches von 3^k, so ändern wir an letzterer Kongruenz nichts. Dies hat zur Folge, daß mit einer Nullstelle x_0 modulo 3^{k+1} auch $x_0 + 3^k$ und $x_0 + 2 \cdot 3^k$ Nullstellen modulo 3^{k+1} sind, wie im Hebungsbaum in §6 gesehen. Man "sieht dort α in jeder Ebene dreifach". Dito β.

Beispiel. Betrachte $u_7(X) = X^6 - 4X^4 - 6X^3 + 5X^2 - 3X - 2$ bei $p = 3$. Es ist die Diskriminante gleich 2489614461, damit $\mathrm{v}_3(2489614461) = 6$ und also brauchen wir eine Genauigkeit von mindestens

$$\mathrm{v}_3(2489614461) + (\deg u_7 - 1)\lfloor \mathrm{v}_3(2489614461)/2 \rfloor + 1 \;=\; 22$$

Stellen. Bei einer Berechnung auf 22 Stellen genau zerfällt $u_7(X)$ in $\mathbf{Z}_3[X]$ in ein Produkt dreier irreduzibler Faktoren vom Grad 2, und bei einer Berechnung auf

$$22 - (3-1) \cdot \lfloor \mathrm{v}_3(2489614461)/2 \rfloor \;=\; 16$$

Stellen genau zerfallen diese nicht weiter. Also haben wir $u_7(X)$ in $\mathbf{Z}_3[X]$ in irreduzible Faktoren zerlegt, und sehen diese in ersterer Berechnung auf 16 Stellen genau.

Im Hebungsbaum in §6 konnten wir ebenfalls keine Nullstelle von $u_7(X)$ in $\mathbf{Z}_3$ erkennen.

Beispiel. Betrachte $u_8(X) = X^6 - X^4 - 6X^3 - 4X^2 + 6X - 5$ bei $p = 3$. Es ist die Diskriminante gleich 8320584384, damit $\mathrm{v}_3(8320584384) = 6$, und also brauchen wir eine Genauigkeit von mindestens

$$\mathrm{v}_3(8320584384) + (\deg u_8 - 1)\lfloor \mathrm{v}_3(8320584384)/2 \rfloor + 1 \;=\; 22$$

Stellen. Bei einer Berechnung auf 22 Stellen genau zerfällt $u_8(X)$ in $\mathbf{Z}_3[X]$ in ein Produkt irreduzibler Faktoren von Grad 1, 1, 2 und 2, und bei einer Berechnung auf

$$22 - (4-1) \cdot \lfloor \mathrm{v}_3(2489614461)/2 \rfloor \;=\; 13$$

Stellen genau zerfallen diese nicht weiter. Also haben wir $u_8(X)$ in $\mathbf{Z}_3[X]$ in irreduzible Faktoren zerlegt, und sehen diese in ersterer Berechnung auf 13 Stellen genau.

Die beiden Linearfaktoren haben wir als Nullstellen von $u_8(X)$ in $\mathbf{Z}_3$ im Hebungsbaum in §6 gesehen.

```
R := pAdicRing(3,22);
P<X> := PolynomialRing(R);
```

```
u8 := P ! X^6-X^4-6*X^3-4*X^2+6*X-5;
fac := Factorisation(u8);
print fac;

R := pAdicRing(3,13);
P<X> := PolynomialRing(R);
Factorisation(P!fac[1][1]);
Factorisation(P!fac[2][1]);
Factorisation(P!fac[3][1]);
Factorisation(P!fac[4][1]);
```

Schreiben wir $u_8(X) = (X-\alpha)(X-\beta)r(X)$ in $\mathbf{Z}_3[X]$, so ist $\alpha \equiv_9 \beta$. Dies hat zur Folge, daß für $k \geqslant 2$ aus $x_0 \equiv_{3^k} \alpha$ immer auch $x_0 \equiv_9 \beta$ folgt, und also $u_6(x_0) \equiv_{3^{k+2}} 0$ gilt. Ändern wir x_0 um ein Vielfaches von 3^k, so ändern wir an $u_6(x_0) \equiv_{3^{k+2}} 0$ nichts. Dies hat zur Folge, daß mit einer Nullstelle x_0 modulo 3^{k+2} auch $x_0 + 3^k$, $x_0 + 2\cdot 3^k$, $\ldots$, $x_0 + 8\cdot 3^k$ Nullstellen modulo 3^{k+2} sind, wie im Hebungsbaum in §6 gesehen. Man "sieht dort α in jeder Ebene neunfach". Dito β.

Zerlege die selbstgefundenen Polynome in $\mathbf{Z}_p[X]$

Vermutlich ergibt sich die Struktur des Hebungsbaums von $f(X) \in \mathbf{Z}[X]$ am besten aus einer Zerlegung von $f(X)$ in Linearfaktoren in $\bar{\mathbf{Q}}_p[X]$ und den Kongruenzen der Nullstellen in $\bar{\mathbf{Q}}_p$ untereinander. Diese Zerlegung existiert, doch das Kongruenzverhalten der Nullstellen untereinander dem Polynom $f(X)$ zu entnehmen, steht auf einem anderen Blatt. Man könnte sich fragen, ob das Newton-Polygon hier hilft.

A Hensel-Koch-Verfahren

Folgende Ausführungen übersteigen den Rahmen des Kurses. Wir folgen **[2,** §4.4].

Sei R ein kompletter diskreter Bewertungsring mit maximalem Ideal erzeugt von $\pi \in R$ und mit Quotientenkörper $K = \operatorname{frac} R$ von Charakteristik 0.

E.g. $R = \mathbf{Z}_p$ und $\pi = p$.

Wir bezeichnen Idealerzeugnisse in $R[X]$ mit spitzen Klammern.

Das Nullpolynom habe Grad $\deg 0 = -\infty$.

A.1 Diskriminante

Sei $f(X) = \sum_{i \geqslant 0} a_i X^i \in R[X]$ ein normiertes Polynom von Grad $n := \deg f$.

Sei L ein Zerfällungskörper von $f(X) \in K[X]$, so daß $L|K$.

Bemerkung [3, II.§2, Prop. 3]. *Der ganze Abschluß S von R in L ist ein diskreter Bewertungsring und ein freier R-Modul von Rang $[S : R] = [L : K]$. Es zerfällt $f(X)$ in $S[X]$ in Linearfaktoren,*

$$f(X) \;=\; \prod_{i \in [1,n]} (X - \alpha_i)\,.$$

Definition. Sei $\Delta(f) := \prod_{i,\, j \in [1,n],\ i<j} (\alpha_i - \alpha_j)^2$ die *Diskriminante* von f. Diese ist invariant unter $\operatorname{Gal}(L|K)$, also in $S \cap K = R$ enthalten.

In Magma erhalten wir die Diskriminante von f mittels `Discriminant(f)`.

Bemerkung. Da $\Delta(f)$ ein symmetrisches Polynom in $\alpha_1, \ldots, \alpha_n$ mit Koeffizienten in $\mathbf{Z}$ ist, ist $\Delta(f)$ auch ein Polynom in $a_1, \ldots, a_n$ mit Koeffizienten in $\mathbf{Z}$ **[5,** §29].

A.2 Resultante

Seien $g(X) = \sum_{i \geqslant 0} b_i X^i$, $h(X) = \sum_{i \geqslant 0} c_j X^j \in K[X]$ gegeben. Schreibe $k := \deg g$ und $\ell := \deg h$.

Definition. Schreibe

$$\operatorname{Result}(g,h) \;:=\; \det \begin{pmatrix} b_0 & b_1 & \ldots & \ldots & b_k & & & \\ & b_0 & b_1 & \ldots & \ldots & b_k & & \\ & & \ddots & & & & \ddots & \\ & & & b_0 & b_1 & \ldots & \ldots & b_k \\ c_0 & c_1 & \ldots & \ldots & c_\ell & & & \\ & c_0 & c_1 & \ldots & \ldots & c_\ell & & \\ & & \ddots & & & & \ddots & \\ & & & c_0 & c_1 & \ldots & \ldots & c_\ell \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\\a\\a\end{matrix}}\right\} \ell \text{ Zeilen} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\\a\\a\end{matrix}}\right\} k \text{ Zeilen} \end{matrix}$$

für die *Resultante* von $g(X)$ und $h(X)$. Es ist also $\operatorname{Result}(g,h) \in R$. Der einzige Summand in der Leibnizformel, der b_0^ℓ enthält, ist $b_0^\ell c_\ell^k$.

Cf. **[5,** §30, §31]. In Magma erhalten wir die Resultante mittels `Resultant(g,h)`.

Lemma. *Seien $g(X) \neq 0$ und $h(X) \neq 0$. Sei L ein Zerfällungskörper von $g(X)h(X) \in K[X]$. Schreibe $g(X) = b_k \prod_{i \in [1,k]} (X - \beta_i)$ und $h(X) = c_\ell \prod_{j \in [1,\ell]} (X - \gamma_j)$ in $L[X]$.*

(1) *Es ist*

$$\mathrm{Result}(g,h) \;=\; b_k^\ell c_\ell^k \prod_{i\in[1,k]} \prod_{j\in[1,\ell]} (\beta_i - \gamma_j)$$

(2) *Es ist*

$$\mathrm{Result}(g,h) \;=\; b_k^\ell \prod_{i\in[1,k]} h(\beta_i)\,.$$

(3) *Es ist*

$$\mathrm{Result}(g,h) \;=\; (-1)^{k\ell} c_\ell^k \prod_{j\in[1,\ell]} g(\gamma_j)\,.$$

Beweis. Es folgen (2) und (3) aus (1). Wir wollen (1) zeigen.

Wir dürfen $g(X)$ und $h(X)$ als normiert annehmen, i.e. $b_k = 1$ und $c_\ell = 1$.

Wir wollen nun stattdessen in $\hat{L} := K[\hat\beta_1\,,\,\ldots\,,\,\hat\beta_k\,,\,\hat\gamma_1\,,\,\ldots\,,\,\hat\gamma_\ell][X]$ für $\hat g(X) := \prod_{i\in[1,k]}(X-\hat\beta_i)$ und $\hat h(X) := \prod_{j\in[1,\ell]}(X-\hat\gamma_j)$ zeigen, daß

$$\mathrm{Result}(\hat g,\hat h) \;\stackrel{!}{=}\; \prod_{i\in[1,k]} \prod_{j\in[1,\ell]} (\hat\beta_i - \hat\gamma_j) \;=:\; P$$

Die Bemerkung wird sich daraus durch Spezialisierung $\hat L \xrightarrow{\sigma} L$, $\hat\beta_i \longmapsto \beta_i$ für $i \in [0,k]$ und $\hat\gamma_j \longmapsto \gamma_j$ für $j \in [0,\ell]$ ergeben.

Wir *behaupten,* daß $(\hat\beta_i - \hat\gamma_j)$ ein Teiler von $\mathrm{Result}(\hat g,\hat h)$ ist für $i \in [1,k]$ und $j \in [1,\ell]$.

Polynomdivision in $K[\hat\beta_1\,,\,\ldots\,,\,\hat\beta_k\,,\,\hat\gamma_1\,,\,\ldots\,,\,\hat\gamma_\ell]$ bezüglich $\hat\beta_i$ gibt

$$\mathrm{Result}(\hat g,\hat h) \;=\; u\cdot(\hat\beta_i - \hat\gamma_j) + v\,,$$

wobei v konstant in $\hat\beta_i$ ist. Spezialisieren wir zu $\hat\beta_i \longmapsto \hat\gamma_j$, so bleibt v ungeändert. Die linke Seite wird jedoch 0, da wir die Gleichung

$$\underbrace{(\hat h/(X-\hat\gamma_j))}_{\deg = \ell-1}\cdot\hat g - \underbrace{(\hat g/(X-\hat\beta_i))}_{\deg = k-1}\cdot\hat h \;=\; 0$$

dann zum Nachweis des Verschwindens der $\mathrm{Result}(\hat g,\hat h)$ definierenden Determinante heranziehen können. Also ist $v = 0$. Dies zeigt die *Behauptung.*

In $\hat L$ ist nach dem Satz von Gauß jedes irreduzible Polynom prim **[5,** §26], wie e.g. $(\hat\beta_i - \hat\gamma_j)$ für $i \in [0,k]$ und $j \in [0,\ell]$. Also teilt P insgesamt $\mathrm{Result}(\hat g,\hat h)$.

Es ist $\mathrm{Result}(\hat g,\hat h)$ ein Polynom in den $\hat\beta_i$, wobei $i \in [1,k]$, mit Koeffizienten in $K[\hat\gamma_1\,,\,\ldots\,,\,\hat\gamma_\ell]$. Als solches hat es gemäß Leibniz Grad $k\ell$ und den Koeffizienten 1 bei $\beta_1^\ell\cdots\beta_k^\ell$. Dies trifft auch auf P zu. Also ist

$$\mathrm{Result}(\hat g,\hat h) \;=\; P\,.$$

□

Korollar. *Seien $g(X)$, $h(X) \in R[X]$ normierte Polynome. Schreibe $k := \deg g$ und $\ell := \deg h$. Es ist*

$$\Delta(gh) \;=\; \Delta(g)\Delta(h)\,\mathrm{Result}(g,h)^2\,.$$

Beweis. Sei L ein Zerfällungskörper für $g(X)h(X) \in K[X]$. Schreibe $g(X) := \prod_{i\in[1,k]}(X-\beta_i)$ und $h(X) := \prod_{j\in[1,\ell]}(X-\gamma_j)$ in $L[X]$. Es wird

$$\begin{aligned}\Delta(gh) &= \Big(\prod_{1\leqslant i<j\leqslant k}(\beta_i-\beta_j)^2\Big)\Big(\prod_{1\leqslant i<j\leqslant \ell}(\gamma_i-\gamma_j)^2\Big)\Big(\prod_{i\in[1,k]}\prod_{j\in[1,\ell]}(\beta_i-\gamma_j)^2\Big)\\ &= \Delta(g)\Delta(h)\operatorname{Result}(g,h)^2\,.\end{aligned}$$

□

Korollar. *Seien $f(X) \in R[X]$ ein normiertes Polynom. Es ist*

$$\Delta(f) = (-1)^{\binom{n}{2}}\operatorname{Result}(f,f')\,.$$

Insbesondere sehen wir abermals, daß $\Delta(f)$ ein ganzzahliges Polynom in den Koeffizienten von f ist.

Beweis. Sei S der ganze Abschluß von R in einem Zerfällungskörper L von $f(X) \in K[X]$. Schreibe $f(X) = \prod_{i\in[1,n]}(X-\alpha_i) \in S[X]$. Es wird

$$f'(X) = \sum_{j\in[1,n]}\prod_{i\in[1,n]\smallsetminus\{j\}}(X-\alpha_i)\,,$$

und also

$$f'(\alpha_j) = \prod_{i\in[1,n]\smallsetminus\{j\}}(\alpha_j-\alpha_i)\,,$$

so daß sich

$$\Delta(f) = (-1)^{\binom{n}{2}}\prod_{j\in[1,n]}f'(\alpha_j) = (-1)^{\binom{n}{2}}\operatorname{Result}(f,f')$$

ergibt. □

Bemerkung. *Seien $f(X)$, $g(X)$, $h(X) \in R[X]$ normierte Polynome mit $f(X) \equiv_{\pi\Delta(f)} g(X)h(X)$. Dann ist*

$$\mathrm{v}_\pi(\operatorname{Result}(g,h)) \leqslant \frac{1}{2}\,\mathrm{v}_\pi(\Delta(f))$$

Beweis. Da die Diskriminante ein ganzzahliges Polynom in den Koeffizienten ihres Arguments ist, ist

$$\Delta(f) \equiv_{\pi\Delta(f)} \Delta(gh) = \Delta(g)\Delta(h)\operatorname{Result}(g,h)^2\,,$$

folglich

$$\mathrm{v}_\pi(\Delta(f)) = \mathrm{v}_\pi\big(\Delta(g)\Delta(h)\operatorname{Result}(g,h)^2\big)$$

und also $\mathrm{v}_\pi(\operatorname{Result}(g,h)^2) \leqslant \mathrm{v}_\pi(\Delta(f))$. □

Satz (Hensel-Koch). *Sei $f(X) \in R[X]$ normiert. Sei $\Delta(f) \neq 0$.*

Schreibe $t := \mathrm{v}_\pi(\Delta(f))$. Schreibe $t' := \lfloor \frac{t}{2} \rfloor = \max\{z \in \mathbf{Z} \,:\, z \leqslant \frac{t}{2}\}$.

Sei $s > t$. Seien $g(X)$, $h(X) \in R[X]$ normiert mit

$$f(X) \equiv_{\pi^s} g(X)h(X)$$

gegeben.

Dann gibt es $\hat{g}(X)$, $\hat{h}(X) \in R[X]$ normiert mit

$$\hat{g}(X) \equiv_{\pi^{s-t'}} g(X)\,, \qquad \hat{h}(X) \equiv_{\pi^{s-t'}} h(X)$$

und mit

$$f(X) = \hat{g}(X)\hat{h}(X)\,.$$

Für diese Verallgemeinerung des üblichen Henselschen Lemmas ist mir als Quelle nur **[2,** Satz 4.4.3] bekannt.

Beweis. Mit Induktion genügt es, $\tilde{g}(X), \tilde{h}(X) \in R[X]$ normiert mit

$$\tilde{g}(X) \stackrel{!}{\equiv}_{\pi^{s-t'}} g(X)\,, \qquad \tilde{h}(X) \stackrel{!}{\equiv}_{\pi^{s-t'}} h(X)$$

und mit

$$f(X) \stackrel{!}{\equiv}_{\pi^{s+1}} \tilde{g}(X)\tilde{h}(X)$$

zu finden.

Wir suchen diese von der Form

$$\begin{aligned} \tilde{g}(X) &= g(X) + \pi^{s-t'}u(X) \\ \tilde{h}(X) &= h(X) + \pi^{s-t'}v(X)\,, \end{aligned}$$

wobei $u(X), v(X) \in R[X]$ mit $\deg u < \deg g$ und $\deg v < \deg h$. Es sollte also

$$\begin{aligned} f(X) &\stackrel{!}{\equiv}_{\pi^{s+1}} (g(X) + \pi^{s-t'}u(X))(h(X) + \pi^{s-t'}v(X)) \\ &= g(X)h(X) + \pi^{s-t'}(v(X)g(X) + u(X)h(X)) + \pi^{2(s-t')}u(X)v(X) \end{aligned}$$

gelten. Beachte, daß $2(s-t') \geqslant s+1$. Schreibe $b(X) := \pi^{t'-s}(f(X) - g(X)h(X)) \equiv_{\pi^{t'}} 0$. Es genügt also, unsere angesetzten $u(X), v(X) \in R[X]$ so zu finden, daß

$$b(X) \stackrel{!}{=} v(X)g(X) + u(X)h(X)\,.$$

Da mit vorstehender Bemerkung $\mathrm{v}_\pi(\mathrm{Result}(g,h)) \leqslant t'$ ist und da $\mathrm{Result}(g,h)$ die Determinante des entstehenden linearen Gleichungssystems für die Koeffizienten von $v(X)$ und $u(X)$ ist, folgt dies mit der Cramerschen Regel, auch als Adjunktenformel bekannt. □

Und jetzt wird es unschön.

Korollar. *Seien $f(X) \in R[X]$ normiert. Sei $\Delta(f) \neq 0$. Schreibe $t := \mathrm{v}_\pi(\Delta(f))$. Schreibe $t' := \lfloor \frac{t}{2} \rfloor$.*

Sei $m \geqslant 2$. Schreibe $t'' := (m-2)t'$.

Sei $s > t + t''$. Für $i \in [1,m]$ seien $g_i(X) \in R[X]$ normiert so gegeben, daß

$$f(X) \equiv_{\pi^s} g_1(X)g_2(X)\cdots g_m(X)\,.$$

Dann gibt es $\hat{g}_i(X) \in R[X]$ normiert mit $\hat{g}_i(X) \equiv_{\pi^{s-t'-t''}} g_i(X)$ für $i \in [1,m]$ und mit

$$f(X) = \hat{g}_1(X)\hat{g}_2(X)\cdots\hat{g}_m(X)\,.$$

Beweis. Induktion über $m \geqslant 2$. Der Induktionsanfang $m = 2$ ist Hensel-Koch.

Induktionsschritt. Sei $m \geqslant 3$. Sei die Aussage für $m-1$ bekannt. Schreibe $h(X) := g_1(X)\cdots g_{m-1}(X)$. Es ist $\Delta(h)$ ein Teiler von $\Delta(f)$.

Es ist

$$f(X) \equiv_{\pi^s} h(X)g_m(X)\,.$$

Dank Hensel-Koch gibt es $\hat{g}_m(X), \hat{h}(X) \in R[X]$ normiert mit

$$\hat{g}_m(X) \equiv_{\pi^{s-t'}} g_m(X)\,, \qquad \hat{h}(X) \equiv_{\pi^{s-t'}} h(X)$$

und mit

$$f(X) \;=\; \hat{h}(X)\hat{g}_m(X)\;.$$

Nun ist

$$\hat{h}(X) \;\equiv_{\pi^{s-t'}}\; h(X) \;=\; g_1(X)\cdots g_{m-1}(X)\;,$$

weswegen es nach Induktionsvoraussetzung $\hat{g}_i(X) \in R[X]$ normiert gibt mit $\hat{g}_i(X) \equiv_{\pi^{(s-t')-t''}} g_i(X)$ für $i \in [1, m-1]$ und mit

$$\hat{h}(X) \;=\; \hat{g}_1(X)\cdots\hat{g}_{m-1}(X)\;.$$

Insgesamt ist also $\hat{g}_i(X) \equiv_{\pi^{s-t'-t''}} g_i(X)$ für $i \in [1, m]$ und

$$f(X) \;=\; \hat{h}(X)\hat{g}_m(X) \;=\; \hat{g}_1(X)\cdots\hat{g}_m(X)\;.$$

□

Anwendung. Sei $f(X) \in \mathbf{Z}[X]$ ein normiertes und rational irreduzibles Polynom mit $\deg f \geqslant 2$. Sei p prim.

Schreibe $t := \mathrm{v}_p(\Delta(f))$. Schreibe $t' := \lfloor \frac{t}{2} \rfloor$. Schreibe $t'' := (\deg f - 2)t'$.

Sei $s > t + t''$.

Sei $m \geqslant 1$ und $g_i(X) \in \mathbf{Z}[X]$ normiert für $i \in [1, m]$ so, daß

$$f(X) \;\equiv_{p^s}\; g_1(X)\cdots g_m(X)$$

eine auch modulo $p^{s-(m-1)t'}$ nicht weiter zerfallende Zerlegung ist. Da $m \leqslant \deg f$, gibt es nach vorstehendem Korollar $\hat{g}_i(X) \in \mathbf{Z}_p[X]$ normiert mit $\hat{g}_i(X) \equiv_{p^{s-(m-1)t'}} g_i(X)$ für $i \in [1, m]$ und

$$f(X) \;=\; \hat{g}_1(X)\cdots\hat{g}_m(X)$$

Für $i \in [1, m]$ ist nun $\hat{g}_i(X)$ irreduzibel in $\mathbf{Z}_p[X]$, denn wäre es etwa für $i = 1$ reduzibel, sagen wir, $\hat{g}_1(X) = u(X)v(X)$ mit $u(X), v(X) \in \mathbf{Z}_p[X]$ normiert von Grad $\geqslant 1$, dann wäre auch $f(X) = u(X)v(X)\hat{g}_2(X)\cdots\hat{g}_m(X) \equiv_{p^{s-(m-1)t'}} u(X)v(X)g_2(X)\cdots g_m(X)$ mit $g_1(X) \equiv_{p^{s-(m-1)t'}} \hat{g}_1(X) = u(X)v(X)$, was nicht geht, da modulo $p^{s-(m-1)t'}$ jedes Polynom in $\mathbf{Z}_p[X]$ von einem Polynom in $\mathbf{Z}[X]$ repräsentiert wird und unsere Zerlegung als nicht weiter zerfallend vorausgesetzt war.

Also sehen wir diesenfalls in der Zerlegung $f(X) \equiv_{p^s} g_1(X)\cdots g_m(X)$ auf s Stellen genau bereits die irreduziblen Faktoren von $f(X)$ in $\mathbf{Z}_p[X]$, aber eben nur bis auf $s-(m-1)t'$ Stellen genau. Die Grade dieser irreduziblen Faktoren in $\mathbf{Z}_p[X]$ können wir jedenfalls ablesen.

> Die Kalamität, modulo $p^{s-(m-1)t'}$ nochmals die weitere Zerlegbarkeit prüfen zu müssen, rührt daher, daß ich nicht die hypothetische Zerlegung $f(X) = u(X)v(X)\hat{g}_2(X)\cdots\hat{g}_m(X)$ modulo p^s direkt mit der Zerlegung $f(X) \equiv_{p^s} g_1(X)\cdots g_m(X)$ dort vergleichen und schon über die Anzahl der Faktoren einen Widerspruch herleiten kann, da in $(\mathbf{Z}/p^s)[X]$ die Eindeutigkeit der Zerlegung in irreduzible Faktoren im allgemeinen nicht gilt. Ich kann auch nicht ausschließen, daß es in $(\mathbf{Z}/p^s)[X]$ zwei nicht weiter zerlegbare Faktorisierungen gibt, in denen die Grade der Faktoren auch bis auf Permutation nicht übereinstimmen.
>
> Gegen die Eindeutigkeit kann man $(X-3)(X+3) \equiv_9 X^2$ anführen. Gegen die Eindeutigkeit der Gradzahlverteilung bis auf Permutation kenne ich kein Beispiel.

Abschließend soll noch ein Ansatz über Linearfaktoren erwähnt werden, vgl. die erste Bemerkung in §A.1.

Bemerkung. *Sei $n \geqslant 1$. Seien $\alpha_i \in R$ für $i \in [1, n]$. Sei $f(X) := \prod_{i\in[1,n]}(X - \alpha_i)$. Sei $t := \mathrm{v}_\pi(\Delta(f))$.*

Sei $s > t$. Sei $s' := \lceil \frac{s}{2} \rceil = \min\{\, z \in \mathbf{Z} \,:\, z \geqslant \frac{s}{2} \,\}$.

Sei $r \in R$ mit $f(r) \equiv_{\pi^s} 0$.

Dann gibt es genau ein $i \in [1, n]$ mit $r \equiv_{\pi^{s'}} \alpha_i$.

Polynomdivision von $f(X)$ durch $(X-r)$ zeigt übrigens, daß $f(r) \equiv_{\pi^s} 0$ gleichbedeutend ist mit $f(X) \equiv_{\pi^s} (X-r)h(X)$ für ein normiertes $h(X) \in R[X]$. Die Bemerkung sagt, daß diesenfalls $f(X) = (X-\alpha_i)\hat{h}(X)$ für ein $i \in [1,n]$ und ein $\hat{h}(X) \in R[X]$ normiert so, daß $(X-r) \equiv_{\pi^{s'}} (X-\alpha_i)$.

Beweis. Zur Existenz. Annahme, $v_i := \mathrm{v}_\pi(r-\alpha_i) \leqslant s'-1$ für $i \in [1,n]$. Sei o.E. $v_1 \leqslant v_2 \leqslant \cdots \leqslant v_n$.

Es ist $s \leqslant \mathrm{v}_\pi(f(r)) = \sum_{i\in[1,n]} v_i$.

Es ist $\alpha_i \equiv_{\pi^{v_i}} r \equiv_{\pi^{v_j}} \alpha_j$ für $1 \leqslant i < j \leqslant n$. Also ist $\alpha_i \equiv_{\pi^{v_i}} \alpha_j$, und somit

$$s \;>\; t \;=\; \mathrm{v}_\pi(\Delta(f)) \;\geqslant\; 2 \sum_{1\leqslant i<j\leqslant n} v_i \;\geqslant\; 2 \sum_{i\in[1,n-1]} v_i \;.$$

Zusammen ist $v_n > \sum_{i\in[1,n-1]} v_i$, und also $2v_n > \sum_{i\in[1,n]} v_i \geqslant s$. Aber $v_n \leqslant s'-1$, und wir haben einen *Widerspruch.*

Zur Eindeutigkeit. Annahme, es gibt $1 \leqslant i < j \leqslant n$ mit $r \equiv_{\pi^{s'}} \alpha_i$ und $r \equiv_{\pi^{s'}} \alpha_j$. Dann ist $\alpha_i - \alpha_j \equiv_{\pi^{s'}} 0$, und also $\mathrm{v}_\pi(\Delta(f)) \geqslant 2s' \geqslant s > t$, was einen *Widerspruch* darstellt. □

Literatur

[1] Bosma, W.; Cannon, J.J.; Fieker, C.; Steel, A. (eds.), *Handbook of Magma functions,* Edition 2.16, 2010; cf. magma.maths.usyd.edu.au, magma.maths.usyd.edu.au/calc.

[2] Koch, H., *Zahlentheorie,* Vieweg, 1997.

[3] Serre, J.-P., *Local Fields*, Springer GTM 67, 1979.

[4] Serre, J.-P., *A Course in Arithmetic,* Springer GTM 7, 5. Aufl., 1996.

[5] van der Waerden, B. L., *Algebra,* Springer Grundlehren, 5. Aufl., 1960.