Lösung Probeklausur Computeralgebra SS15

Max Berrendorf Michael Ellers Joel Hermanns Christopher Hugenroth
Peter Sommerhoff

4. August 2015

Das vorliegende Dokument ist eine von uns erstellte Lösung zu der Probeklausur im Fach Computeralgebra im Sommersemester 2015. Sie stellt keinen Anspruch auf Korrektheit oder Vollständigkeit. Insbesondere wurde sie weder von Prof. Dr. Gabriele Nebe, ihrem Lehrstuhl noch ihren Mitarbeitern erstellt oder geprüft.

Aufgabe 1.

Es sei $G := \langle a := (1,2,3,4,5,6,7), b := (2,3,5)(4,7,6) \rangle \leq \mathrm{S}_7$.

1. Bestimmen Sie $|G|$.

Nutze den base-and-strong-generator-Algorithmus zur Bestimmung einer base sowie eines starken Erzeugendensystems. Beginne mit $G_1 1$ (siehe Abbildung **??**) mit $G_1 := G$. Für das Erzeugendensystem von $G_2 := \mathrm{Stab}_{G_1}(1)$ ergibt sich

$$G_2 = \left\langle b, a^{-2}ba, a^{-2}b^{-1}a^4, a^{-1}b^2a^2, a^{-3}baba^2, aba^3, a^{-2}b^{-1}a^{-1}b^2a^3 \right\rangle$$

Es gilt

- $a^2 = (1,3,5,7,2,4,6), a^{-2} = (1,6,4,2,7,5,3)$,
- $ba = (2,3,5)(4,7,6)(1,2,3,4,5,6,7) = (1,3,7)(2,5,4)$,
- $a^{-2}ba = a^5ba = (1,6,4,2,7,5,3)(1,3,7)(2,5,4) = b \iff ba = a^2b$,
- $aba^3 = abaaa = aaabaa = aaaaaba = aaaaaaab = b$,
- $a^{-2}b^{-1}a^4 = a^5bba^4 = a^5bab = b^2$,
- $a^{-1}b^2a^2 = a^6bba^2 = a^6ba^4b = b^2$,
- $a^{-1}b^2a^2 = a^{-1}ba^4b = b^2$,
- $a^{-2}b^{-1}a^{-1}b^2a^3 = a^5bba^6bba^3 = aba^2ba^6bba^3 = aba^3 = b$.

Somit gilt $G_2 = \langle b \rangle$. Nun berechne $G_2 2$ (siehe Abbildung **??**). Es gilt $\mathrm{Stab}_{G_2}(2) = \{\mathrm{id}\}$. Insgesamt folgt

$$|G| = |G_1 1| \cdot |G_2 2| = 7 \cdot 3 = 21$$

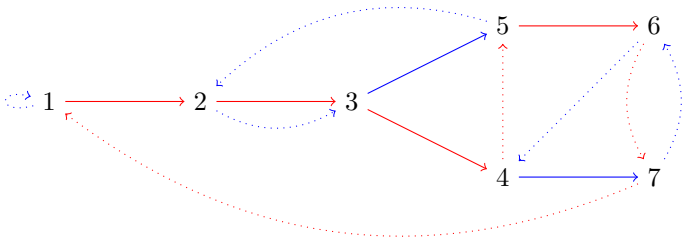

Abbildung 1: Bahn von G_1 auf 1. Blaue Pfeile sind Multiplikation mit b, rote Pfeile Multiplikation mit a.

2. Liegt die Permutation $g := (1,3,4)(2,7,6)$ in G?

Eine base ist $(1,2)$ mit zugehörigen starken Erzeugern

1	2	3	4	5	6	7
id	a	a^2	a^3	ba^2	aba^2	ba^3
	id	b		b^2		

Es gilt

$$g1 = (1,3,4)(2,7,6)1 = 3 = a^2 1 \in G_1 1 \implies \left(g \in G \iff a^{-2}g \in G_2\right)$$

Es ist $a^{-2}g = (1,6,4,2,7,5,3)(1,3,4)(2,7,6) = (1)(2,5,3)(4,6,7) = b \in G_2$. Also ist $g \in G$.

3. Liegt die Permutation $h := (1,3,2,5,4,6,7)$ in G?

Es gilt

$$h1 = (1,3,4)(2,7,6)1 = 3 = a^2 1 \in G_1 1 \implies \left(h \in G \iff a^{2-}h \in G_2\right)$$

Es ist $a^{-2}h = (1,6,4,2,7,5,3)(1,3,2,5,4,6,7) = (1)(2,3,7,6,5)(4)$ und weiter

$$a^{-2}h2 = (2,3,7,6,5)2 = 3 \in G_2 2 \implies \left(a^{-2}h \in G_2 \iff b^{-1}a^2 h \in G_3 = \{\mathrm{id}\}\right)$$

Es ist $b^{-1}a^{-2}h2 = 5 \neq 2 \implies b^{-1}a^{-2}h \neq \mathrm{id}$. Also ist $h \notin G$.

Aufgabe 2.

1. Definieren Sie den Begriff der transitiven G-Menge.

Eine Gruppe G operiere auf einer Menge M. M ist eine transitive G-Menge, falls $M = Gm$ für ein $m \in M$. (Vgl. Skript: Definition 1.16(b))

2. Definieren Sie Äquivalenz von G-Mengen.

Sei G eine Gruppe, M, N zwei G-Mengen. Dann heißen M und N äquivalent (bzw. ähnlich), falls es eine G-äquivariante Bijektion $\varphi : M \to N$ gibt, d.h. $\varphi(gm) = g\varphi(m)$ für alle $m \in M$. (Vgl. Skript: Definition 1.24)

3. Formulieren Sie den Klassifikationssatz über transitive G-Mengen.

Sei G Gruppe. Die G-Ähnlichkeitsklassen der transitiven G-Mengen und die Konjugiertenklassen der Untergruppen von G stehen in Bijektion: $\varphi : U \mapsto G/U$. (Vgl. Skript: Hauptsatz 1.26 (4)).

4. Wieviele Äquivalenzklassen transitiver G-Mengen gibt es für $G = \mathrm{A}_4$

Der Untergruppenverband der $\mathrm{A}_4 = \langle a := (1,2,3), b := (2,3,4)\rangle$ ist in Abbildung **??** abgebildet. Mit dem Klassifikationssatz für transitive G-Mengen folgt damit, dass es bis auf Ähnlichkeit 5 transitive G-Mengen gibt.

Aufgabe 3.

1. Formulieren Sie das Burnsidesche Fixpunktlemma.

Eine endliche Gruppe G operiere auf einer ebenfalls endlichen Menge M. Für $g \in G$ definiere

$$\mathrm{fix}(g) := |\{m \in M \mid gm = m\}|.$$

Dann lässt sich die Anzahl der Bahnen von G auf M berechnen durch

$$|G\backslash M| = \frac{1}{|G|}\sum_{g \in G} \mathrm{fix}(g)$$

(Vgl. Skript: Satz 1.42).

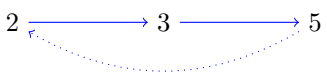

Abbildung 2: Bahn von G_2 auf 1. Blaue Pfeile sind Multiplikation mit b, rote Pfeile Multiplikation mit a.

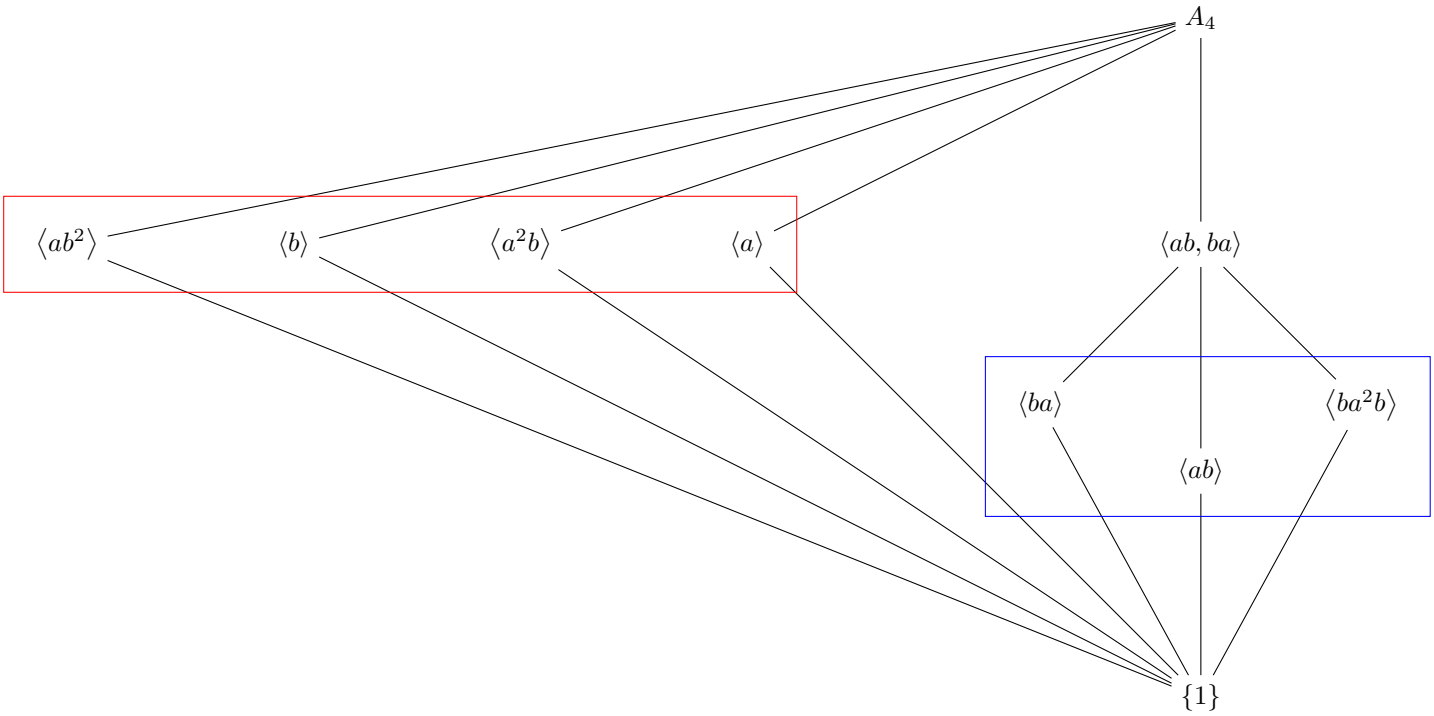

Abbildung 3: Untergruppenverband von $A_4 = \langle a := (1,2,3), b := (2,3,4) \rangle$. Die Kästen indizieren Konjugiertenklassen.

2. Wieviele echt verschiedene Graphen auf 4 Punkten gibt es?

Graphen auf 4 Punkten können durch die Menge der Funktionen $M := \{f : \mathrm{Pot}_2(\underline{4}) \to \{0,1\}\}$ modelliert werden. Zwei Graphen sind echt verschieden, wenn sie nicht durch eine bijektive Abbildung aufeinander abgebildet werden, d.h. nicht in der gleichen Bahn bezüglich der Operation der S_4 liegen. Die S_4 operiert auf der Menge der Pot_2 und damit auch auf M. Es gilt

Vertreter der Konjugiertenklasse	$\lvert KK \rvert$	Operation auf $\mathrm{Pot}_2(\underline{4})$	$\mathrm{fix}_M(g)$
id	1	$\mathrm{id}_{\mathrm{Pot}_2(\underline{4})}$	2^6
(1,2)	6	$(\{1,2\})(\{1,3\},\{2,3\})(\{1,4\},\{2,4\})(\{3,4\})$	2^4
(1,2)(3,4)	3	$(\{1,2\})(\{1,3\},\{2,4\})(\{1,4\},\{2,3\})(\{3,4\})$	2^4
(1,2,3)	8	$(\{1,2\},\{2,3\},\{1,3\})(\{1,4\},\{2,4\},\{3,4\})$	2^2
(1,2,3,4)	6	$(\{1,2\},\{2,3\},\{3,4\},\{1,4\})(\{1,3\},\{2,4\})$	2^2

Mit dem Burnsideschen Fixpunktlemma folgt

$$\begin{aligned}
|M \backslash \mathrm{S}_4| &= \frac{1}{|S_4|} \sum_{\sigma \in \mathrm{S}_4} \mathrm{fix}_M(\sigma) \\
&= \frac{1}{24} \left(2^6 + 6 \cdot 2^4 + 3 \cdot 2^4 + 8 \cdot 2^2 + 6 \cdot 2^2\right) \\
&= \frac{1}{2^3 \cdot 3} \left(2^6 + 3 \cdot 2^5 + 3 \cdot 2^4 + 2^5 + 2 \cdot 2^3\right) \\
&= \frac{1}{2^3 \cdot 3} \left(3 \cdot 2^5 + 3 \cdot 2^5 + 3 \cdot 2^4 + 2 \cdot 2^3\right) \\
&= 2^2 + 2^2 + 2 + 1 \\
&= 11
\end{aligned}$$

Aufgabe 4.

1. Formulieren Sie die Sylowsätze.

Sei G eine endliche Gruppe und p eine Primzahl.

1. $$\left|\mathrm{Syl}_p(G)\right| \equiv 1 \pmod{p}.$$

   Insbesondere existiert mindestens eine Sylowuntergruppe von G.

2. Sei $U \leq G$, $|U| = p^\beta$, $P \in \mathrm{Syl}_p(G)$. Dann existiert ein $g \in G$, so dass ${}^gU \leq P \in \mathrm{Syl}_p(G)$. Insbesondere ist jede maximale p-Untergruppe von G eine p-Sylowuntergruppe von G.

3. Alle p-Sylowuntergruppen von G sind konjugiert in G. Insbesondere gilt $\mathrm{Syl}_p(G) \equiv G/\mathrm{N}_G(P)$, $P \in \mathrm{Syl}_p(G)$ als G-Menge ($\equiv$ bezeichnet hierbei die Ähnlichkeit von G-Mengen) und $\left|\mathrm{Syl}_p(G)\right| \mid |G|$, sogar $\left|\mathrm{Syl}_p(G)\right| \mid \frac{|G|}{|P|}$.

(Vgl. Skript: Hauptsatz 1.49)

2. Bestimmen Sie bis auf Isomorphie alle Gruppen der Ordnung 99.

Es gilt $99 = 3^2 \cdot 11$. Mit den Sylowsätzen folgt:

- $|\mathrm{Syl}_3(G)| \equiv_3 1$ und
- $|\mathrm{Syl}_3(G)| \mid \frac{|G|}{3^2} = 11$.

$\Longrightarrow$ $|\mathrm{Syl}_3(G)| = 1$. Sei $P \in \mathrm{Syl}_3(G)$, dann gilt also $P \trianglelefteq G$. Weiterhin folgt mit den Sylowsätzen:

- $|\mathrm{Syl}_{11}(G)| \equiv_{11} 1$ und
- $|\mathrm{Syl}_{11}(G)| \mid \frac{|G|}{11} = 9$.

$\Longrightarrow$ $|\mathrm{Syl}_{11}(G)| = 1$. Sei $Q \in \mathrm{Syl}_{11}(G)$, dann gilt also $Q \trianglelefteq G$. Da $P \cap Q = \{1\}$ aus Ordnungsgründen, gilt also $G \cong P \times Q$. Für P gibt es die Möglichkeiten $P \cong \mathrm{C}_3 \times \mathrm{C}_3$ oder $P \cong \mathrm{C}_9$; $Q \cong \mathrm{C}_{11}$ gilt stets. Somit sind $G \cong \mathrm{C}_{11} \times \mathrm{C}_9$ oder $G \cong \mathrm{C}_{11} \times \mathrm{C}_3 \times \mathrm{C}_3$ die einzigen Möglichkeiten.

Aufgabe 5.

1. Definieren Sie die folgenden Begriffe: Normalteiler einer Gruppe, charakteristische Untergruppe, Kommutatoruntergruppe.

Normalteiler einer Gruppe Eine Untergruppe N der Gruppe G heißt Normalteiler von G (Bezeichnung $N \trianglelefteq G$), falls

$$N = {}^gN = gNg^{-1} \text{ für alle } g \in G$$

(Vgl. Skript: Definition 1.50)

Charakteristische Untergruppe Eine Untergruppe $U \leq G$ heißt charakteristische Untergruppe von G falls $\alpha(U) = U$ für alle $\alpha \in \mathrm{Aut}(G)$. (Vgl. Skript: Definition 1.59)

Kommutatoruntergruppe Sei G eine Gruppe. Für $a, b \in G$ heißt $[a,b] := a^{-1}b^{-1}ab$ der Kommutator von a, b. Die von allen Kommutatoren erzeugte Untergruppe heißt Kommutatoruntergruppe von G. Bezeichnung: $G' = \langle [a,b] \mid a, b \in G \rangle$. (Vgl. Skript: Definition 1.65)

2. Es sei G eine Gruppe und $U \leq G$ mit $G' \leq U$. Zeigen Sie, dass $U \trianglelefteq G$. Ist U sogar stets charakterisch in G?

Es gilt für alle $g \in G$:

$$gUg^{-1} := \left\{gug^{-1} \mid u \in U\right\} \overset{G' \leq U}{=} \left\{g[g,u]ug^{-1} \mid u \in U\right\} = \left\{ugg^{-1} \mid u \in U\right\} = \{u \mid u \in U\} = U$$

Somit ist $U \trianglelefteq G$.

Die Obergruppen von G' sind nicht notwendigerweise charakteristisch. Das kleinste Gegenbeispiel sind die Untergruppen isomorph zu C_2 in einer Gruppe G isomorph zu $\mathrm{C}_2 \times \mathrm{C}_2$. Die Gruppe G ist abelsch, also ist $G' = \{1\}$; die Automorphismengruppe ist isomorph zu $\mathrm{GL}_2(2)$ und operiert transitiv auf den Untergruppen von Ordnung 2.

Aufgabe 6.

Es sei $G := \left\langle a, b \mid a^4, b^3, a^2b = ba^2 \right\rangle = \left\langle a, b \mid a^4, b^3, a^2ba^{-2}b^{-1} \right\rangle$.

1. Bestimmen Sie die Invariantenteiler von G/G'.

	a^4G'	b^3G'	$a^2ba^{-2}b^{-1}G'$
a	4	0	0
b	0	3	0

Bestimme also die Smith-Normalform der Matrix

$$\begin{pmatrix}4&0&0\\0&3&0\end{pmatrix} \rightsquigarrow \begin{pmatrix}4&-3&0\\0&3&0\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&-3&0\\3&3&0\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&0&0\\3&12&0\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&0&0\\0&12&0\end{pmatrix}$$

Der einzige Invariantenteiler ist also 12.

2. Zeigen Sie, dass es einen surjektiven Gruppenhomomorphismus $G \to \mathrm{S}_3$ gibt.

Betrachte $\varphi : G \to \mathrm{S}_3$ mit $\varphi(a) := (1,2)$ und $\varphi(b) := (1,2,3)$. Dann gilt:

- $\varphi(a)^4 = ((1,2))^4 = 1_{\mathrm{S}_3}$,
- $\varphi(b)^3 = ((1,2,3))^3 = 1_{\mathrm{S}_3}$, und
- $\varphi(a)^2\varphi(b) = ((1,2))^2(1,2,3) = (1,2,3) = (1,2,3)((1,2))^2 = \varphi(b)\varphi(a)^2$.

$\implies$ φ ist Homomorphismus.
Weiterhin gilt: $\langle \varphi(a), \varphi(b)\rangle = \langle (1,2), (1,2,3)\rangle = \mathrm{S}_3$. $\implies$ φ surjektiv.

Aufgabe 7.

1. Formulieren Sie den chinesischen Restsatz.

Sei R ein Ring und $I_1, \ldots, I_n$ paarweise teilerfremde Ideale von R, d. h. $I_i \trianglelefteq R$ und $I_i + I_j = R$ für $i, j = 1, \ldots, n$ mit $i \neq j$. Dann gilt:

$$R/\bigcap_{i=1}^{n} I_i \to \bigoplus_{i=1}^{n} R/I_i, \qquad r + \bigcap_{i=1}^{n} I_i \mapsto (r + I_1, \ldots, r + I_n)$$

ist Isomorphismus. (Vgl. Skript: Satz 2.20)

2. Bestimmen Sie die Lösung kleinsten Grades des folgenden Kongruenzensystems über $\mathbb{Q}[x]$

$$\begin{aligned} f &\equiv -x + 1 \pmod{x^2+1} \\ f &\equiv x + 1 \pmod{x^2-1} \\ f &\equiv 3x - 1 \pmod{x^2+x-2} \end{aligned}$$

Es gilt $x^2 - 1 = (x+1)(x-1)$ und $\mathrm{ggT}(x+1, x-1) \in (\mathbb{Q}[x])^* = \mathbb{Q}^*$, denn

$$\begin{array}{r} (x+1) : (x-1) = 1 \\ -(x-1) \\ \hline 2 \end{array}$$

und $2 \in \mathbb{Q}^*$. Außerdem gilt $\left(x^2+x+2\right) = (x+2)(x-1)$ und $\mathrm{ggT}(x+2, x-1) \in (\mathbb{Q}[x])^* = \mathbb{Q}^*$, denn

$$\begin{array}{r} (x+2) : (x-1) = 1, \text{ Rest: } 3 \\ -(x-1) \\ \hline 3 \end{array}$$

und $3 \in \mathbb{Q}^*$. Mit dem Chinesischen Restsatz folgt also

$$\begin{aligned} f &\equiv -x + 1 \pmod{x^2+1} \\ f &\equiv 0 \pmod{x+1} \\ f &\equiv 2 \pmod{x-1} \\ f &\equiv -7 \pmod{x+2} \\ (f &\equiv 2 \pmod{x-1}) \end{aligned}$$

Euklidischer Algorithmus I Berechne zuerst ggT $\left(x^2+1,(x+1)(x-1)(x+2)\right)$ mittels des erweiterten euklidischen Algorithmus. Es gilt

$$(x+1)(x-1)(x+2) = x^3+2x^2-x-2.$$

Damit folgt

$$\begin{array}{r}
\left(x^3+2x^2-x-2\right) : \left(x^2+1\right) = x+2, \text{ Rest: } -2x-4 \\
-\left(x^3-x\right) \\
\hline
2x^2-2x-2 \\
-\left(2x^2+2\right) \\
\hline
-2x-4
\end{array}$$

Da $-2x-4 \notin (\mathbb{Q}[x])^*$, fahre fort:

$$\begin{array}{r}
\left(x^2+1\right) : (-2x-4) = -\frac{1}{2}x+1, \text{ Rest: } 5 \\
-\left(x^2+2x\right) \\
\hline
-2x+1 \\
-(-2x-4) \\
\hline
5
\end{array}$$

Da $5 \in (\mathbb{Q}[x])^*$ gilt ggT $\left(x^2+1,(x+1)(x-1)(x+2)\right) = 5$ und die Bézout-Identität ergibt

$$\begin{aligned}
5 &= \left(x^2+1\right) - \left(-\frac{1}{2}x+1\right)(-2x-4) \\
&= \left(x^2+1\right) - \left(-\frac{1}{2}x+1\right)\left(\left(x^3+2x^2-x-2\right) - \left(x^2+1\right)(x+2)\right) \\
&= \left(-\frac{1}{2}x^2+3\right)\left(x^2+1\right) + \left(\frac{1}{2}x-1\right)\left((x+1)(x-1)(x+2)\right)
\end{aligned}$$

und damit

$$1 = \frac{1}{5}\left(-\frac{1}{2}x^2+3\right)\left(x^2+1\right) + \frac{1}{5}\left(\frac{1}{2}x-1\right)\left((x+1)(x-1)(x+2)\right).$$

Euklidischer Algorithmus II Nun berechne ggT $\left(x-1,\left(x^2+1\right)(x+1)(x+2)\right)$ mittels des erweiterten euklidischen Algorithmus. Es gilt

$$\left(x^2+1\right)(x+1)(x+2) = x^4+3x^3+3x^2+3x+2.$$

Damit folgt

$$\begin{array}{r}
\left(x^4+3x^3+3x^2+3x+2\right) : (x-1) = x^3+4x^2+7x+10, \text{ Rest: } 12 \\
-\left(x^4-x^3\right) \\
\hline
4x^3+3x^2+3x+2 \\
-\left(4x^3-4x^2\right) \\
\hline
7x^2+3x+2 \\
-\left(7x^2-7x\right) \\
\hline
10x+2 \\
-(10x-10) \\
\hline
12
\end{array}$$

Da $12 \in (\mathbb{Q}[x])^*$ gilt ggT $\left(x-1,\left(x^2+1\right)(x+1)(x+2)\right) = 12$ und die Bézout-Identität ergibt

$$12 = -\left(x^3+4x^2+7x+10\right)(x-1) + 1 \cdot \left(\left(x^2+1\right)(x+1)(x+2)\right)$$

und damit

$$1 = -\frac{1}{12}\left(x^3+4x^2+7x+10\right)(x-1) + \frac{1}{12}\left(\left(x^2+1\right)(x+1)(x+2)\right)$$

Euklidischer Algorithmus III Zuletzt berechne ggT $\left(x+2,\left(x^2+1\right)(x+1)(x-1)\right)$ mittels des erweiterten euklidischen Algorithmus. Es gilt

$$\left(x^2+1\right)(x+1)(x-1) = x^4-1.$$

Damit folgt

$$
\begin{array}{r}
\left(x^4-1\right) : (x+2) = x^3 - 2x^2 + 4x - 8, \text{ Rest: } 15 \\
-\left(x^4+2x^3\right) \\
\hline
-2x^3 - 1 \\
-\left(-2x^3-4x^2\right) \\
\hline
4x^2 - 1 \\
-\left(4x^2+8x\right) \\
\hline
-8x - 1 \\
-(-8x-16) \\
\hline
15
\end{array}
$$

Da $15 \in (\mathbb{Q}[x])^*$ gilt $\operatorname{ggT}\left(x+2, \left(x^2+1\right)(x+1)(x-1)\right) = 15$ und die Bézout-Identität ergibt

$$15 = -\left(x^3 - 2x^2 + 4x - 8\right)(x+2) + 1 \cdot \left(\left(x^2+1\right)(x+1)(x-1)\right)$$

und damit

$$1 = -\frac{1}{15}\left(x^3 - 2x^2 + 4x - 8\right)(x+2) + \frac{1}{15}\left(\left(x^2+1\right)(x+1)(x-1)\right)$$

Zusammensetzen der Lösung Mit dem chinesischen Restsatz folgt für die Lösung:

$$
\begin{aligned}
f &= (-x+1) \cdot \frac{1}{5}\left(\frac{1}{2}x - 1\right)((x+1)(x-1)(x+2)) \\
&\quad + 2 \cdot \frac{1}{12}\left(\left(x^2+1\right)(x+1)(x+2)\right) \\
&\quad + (-7) \cdot \frac{1}{15}\left(\left(x^2+1\right)(x+1)(x-1)\right) \\
&\quad + \left\langle \left(x^2+1\right)(x+1)(x-1)(x+2) \right\rangle \\
&= -\frac{1}{10}x^5 + \frac{1}{10}x^4 + \frac{1}{2}x^3 - \frac{1}{2}x^2 - \frac{2}{5}x + \frac{2}{5} \\
&\quad + \frac{1}{6}x^4 + \frac{1}{2}x^3 + \frac{1}{2}x^2 + \frac{1}{2}x + \frac{1}{3} \\
&\quad - \frac{7}{15}x^4 + \frac{7}{15} + \left\langle x^5 + 2x^4 - x - 2 \right\rangle \\
&= -\frac{1}{10}x^5 - \frac{1}{5}x^4 + x^3 + \frac{1}{10}x + \frac{6}{5} + \left\langle x^5 + 2x^4 - x - 2 \right\rangle
\end{aligned}
$$

Reduzieren der Lösung Die kleinste Lösung ergibt sich nun als Rest der Polynomdivision von $-\frac{1}{10}x^5 - \frac{1}{5}x^4 + x^3 + \frac{1}{10}x + \frac{6}{5}$ durch $x^5 + 2x^4 - x - 2$:

$$
\begin{array}{r}
\left(-\frac{1}{10}x^5 - \frac{1}{5}x^4 + x^3 + \frac{1}{10}x + \frac{6}{5}\right) : \left(x^5 + 2x^4 - x - 2\right) = -\frac{1}{10}, \text{ Rest: } x^3 + 1 \\
-\left(-\frac{1}{10}x^5 - \frac{1}{5}x^4 + \frac{1}{10}x + \frac{1}{5}\right) \\
\hline
x^3 + 1
\end{array}
$$

Somit ist die kleinste Lösung gegeben durch $x^3 + 1$.

Aufgabe 8.

1. Definieren Sie den Begriff Primelement in einem Ring R.

Sei R ein Integritätsbereich. Ein Element $0 \neq a \in R - R^*$ heißt prim, falls gilt:

$$a \mid (b_1 b_2) \implies a \mid b_1 \text{ oder } a \mid b_2 \text{ für alle } b_i \in R.$$

(Vgl. Skript: Definition 2.29(2))

2. Definieren Sie den Begriff irreduzibles Element in einem Ring R.

Sei R ein Integritätsbereich. Ein Element $0 \neq a \in R - R^*$ heißt irreduzibel, falls jede Faktorisierung von a in R trivial ist, das heißt, falls gilt:

$$a = a_1 a_2, \quad a_i \in R \implies a_1 \in R^* \text{ oder } a_2 \in R^*.$$

(Vgl. Skript: Definition 2.29(1))

3. Zeigen Sie, dass $2 \in \mathbb{Z}\left[\sqrt{-5}\right]$ irreduzibel aber nicht prim ist.

$2 \in \mathbb{Z}\left[\sqrt{-5}\right]$ **ist nicht prim.** Es gilt $2 \mid 3 \cdot 2 = \left(1-\sqrt{-5}\right)\left(1+\sqrt{-5}\right)$, aber $2 \nmid \left(1-\sqrt{-5}\right)$ und $2 \nmid \left(1+\sqrt{-5}\right)$.

$2 \in \mathbb{Z}\left[\sqrt{-5}\right]$ **irreduzibel.** Nach Skript.

Aufgabe 9.

1. Formulieren Sie Eisensteinsche Irreduzibilitätskriterium.

R sei faktoriell, K Quot (R) und $f(x) = a_n x^n + \ldots + a_0 \in R[x]$ mit $a_n \neq 0$ und $n > 0$. Sei weiter $p \in R$ prim, so dass $p \nmid a_n$ und $p \mid a_i$ für $i = n-1, \ldots, 0$ und $p^2 \nmid a_0$. Dann ist $f(x)$ irreduzibel in $K[x]$. (Vgl. Skript: Satz 2.40)

2. Zeigen Sie, dass $f(x) = x^8 + 13x^3 - 169x^2 + 26 \in \mathbb{Z}[x]$ irreduzibel ist.

Es gilt:

- $\mathbb{Z}$ faktoriell.
- $n = \deg(f) = 8 > 0$ und somit $a_n = a_8 \neq 0$.
- $p = 13 \in \mathbb{Z}$ prim mit
  - $13 \nmid a_n = 1$,
  - $13 \mid 0, 0, 0, 0, 13, -169, 0, 26 \implies \forall 0 \leq i < n : \ p \mid a_i$.
  - $13^2 \nmid a_0 = 26$.

Damit sind alle Voraussetzung des Eisensteinkriteriums erfüllt und es folgt, dass $f(x)$ irreduzibel über Quot $(\mathbb{Z})[x] = \mathbb{Q}[x]$ ist. Weiterhin ist $f(x)$ normiert, also insbesondere primitiv. Somit folgt mit dem Gaußschen Lemma, dass $f(x)$ auch über $\mathbb{Z}[x]$ irreduzibel ist.

3. Zeigen Sie, dass $f(x) = x^5 + 9x^3 - 27x^2 + 9 \in \mathbb{Z}[x]$ irreduzibel ist.

Es gilt:

- $\mathbb{Z}$ faktoriell.
- $\deg(f) = 5 = 2 \cdot 2 + 1 > 0$ und $a_{2n+1} = a_5 = 1 \neq 0$.
- $p = 3 \in \mathbb{Z}$ prim mit
  - $3 \nmid a_{2n+1} = 1$,
  - $3 \nmid 0, 9 \implies \forall n < i \leq 2n : \ p \mid a_i$,
  - $3^2 \mid 27, 0 \implies \forall 0 < i \leq n : \ p^2 \mid a_i$,
  - $3^3 \nmid a_0 = 9$.

Somit sind alle Voraussetzungen der Variante des Eisensteinkriteriums (vgl. Übung 8, Aufgabe 6) erfüllt und es folgt, dass $f(x)$ irreduzibel über Quot $(\mathbb{Z})[x] = \mathbb{Q}[x]$ ist. Weiterhin ist $f(x)$ normiert, also insbesondere primitiv. Somit folgt mit dem Gaußschen Lemma, dass $f(x)$ auch über $\mathbb{Z}[x]$ irreduzibel ist.

Aufgabe 10.

1. Formulieren Sie einen Algorithmus, der zu einem gegebenen Polynom $f \in \mathbb{F}_p[x]$ das Produkt g aller irreduziblen Teiler von f vom Grad i bestimmt.

Siehe Skript.

2. Bestimmen Sie alle irreduziblen Teiler von $f := x^8+x^7+x^5+x^4+x^3+1 \in \mathbb{F}_2[x]$ vom Grad kleiner oder gleich 2.

Es ist

$$f' = 8x^7 + 7x^6 + 5x^4 + 4x^3 + 3x^2 \equiv_2 x^6 + x^4 + x^2$$

Berechne $\mathrm{ggT}\,(f, f')$.

$$\begin{array}{r}
\left(x^8+x^7+x^5+x^4+x^3+1\right) : \left(x^6+x^4+x^2\right) = x^2+x, \text{ Rest: } 1 \\
-\left(x^8+x^6+x^4\right) \\
\hline
x^7+x^5+x^3+1 \\
-\left(x^7+x^5+x^3\right) \\
\hline
1
\end{array}$$

Da $\mathrm{ggT}\,(f, f') = 1$, ist f quadratfrei. Berechne nun alle irreduziblen Teiler vom Grad $j = 1$. Dazu berechne $\mathrm{ggT}\left(f, x^{(2^1)} - x\right)$:

$$\begin{array}{r}
\left(x^8+x^7+x^5+x^4+x^3+1\right) : \left(x^2+x\right) = x^6+x^3+x+1, \text{ Rest: x+1} \\
-\left(x^8+x^7\right) \\
\hline
x^5+x^4+x^3+1 \\
-\left(x^5+x^4\right) \\
\hline
x^3+1 \\
-\left(x^3+x^2\right) \\
\hline
x^2+1 \\
-\left(x^2+x\right) \\
\hline
x+1
\end{array}$$

Da $x+1 \notin (\mathbb{F}_2[x])^* = \mathbb{F}_2^*$, fahre fort.

$$\begin{array}{r}
\left(x^2+x\right) : (x+1) = x, \text{ Rest: x+1} \\
-\left(x^2+x\right) \\
\hline
0
\end{array}$$

Also ist $\mathrm{ggT}\left(f, x^{(2^1)} - x\right) = x+1 =: f_1$. Da $\deg(f_1) = 1$, ist dies bereits der einzige irreduzible Teiler vom Grad 1. Fahre nun fort mit $g := f/f_1$:

$$\begin{array}{r}
\left(x^8+x^7+x^5+x^4+x^3+1\right) : (x+1) = x^7+x^4+x^2+x+1 \\
-\left(x^8+x^7\right) \\
\hline
x^5+x^4+x^3+1 \\
-\left(x^5+x^4\right) \\
\hline
x^3+1 \\
-\left(x^3+x^2\right) \\
\hline
x^2+1 \\
-\left(x^2+x\right) \\
\hline
x+1 \\
-(x+1) \\
\hline
0
\end{array}$$

Also $g = x^7+x^4+x^2+x+1$. Berechne nun alle irreduziblen Teiler vom Grad $j = 2$. Dazu berechne $\mathrm{ggT}\left(f, x^{(2^2)} - x\right)$:

$$\begin{array}{r}
\left(x^7+x^4+x^2+x+1\right) : \left(x^4+x\right) = x^3, \text{ Rest: } x^2+x+1 \\
-\left(x^7+x^4\right) \\
\hline
x^2+x+1
\end{array}$$

Da $x^2+x+1 \notin (\mathbb{F}_2[x])^* = \mathbb{F}_2^*$, fahre fort.

$$\begin{array}{r}
\left(x^4+x\right) : \left(x^2+x+1\right) = x^2+x, \text{ Rest: } 0 \\
-\left(x^4+x^3+x^2\right) \\
\hline
x^3+x^2+x \\
-\left(x^3+x^2+x\right) \\
\hline
0
\end{array}$$

Also ist $\mathrm{ggT}\left(f, x^{(2^2)} - x\right) = x^2+x+1 =: f_2$. Da $\deg(f_2) = 2$, ist dies bereits der einzige irreduzible Teiler vom Grad 2.

Aufgabe 11.

1. Definieren Sie den Begriff der Termordnung.

Sei $R := K[x_1, \ldots, x_n]$ Eine Termordnung ist eine lineare Ordnung $<$ auf $\mathrm{Mon}(R)$ mit

1. $v < x_i v$ für alle $v \in \mathrm{Mon}(R)$ und alle $1 \leq i \leq n$ und
2. $v < w \implies x_i v < x_i w$ für alle $v, w \in \mathrm{Mon}(R)$ und alle $1 \leq i \leq n$.

(Vgl. Skript: Definition 3.17)

2. Ordnen Sie die folgenden Monome in $\mathrm{Mon}(K[x_1, x_2])$ bezüglich der lexikographischen Termordnung mit $x_1 > x_2$:

$$x_1^3 x_2^4, \quad x_1 x_2^7, \quad x_1^3 x_2^5, \quad x_1^2 x_2.$$

Es gilt

Monom	Tupelschreibweise
$x_1^3 x_2^4$	(3,4)
$x_1 x_2^7$	(1,7)
$x_1^3 x_2^5$	(3,5)
$x_1^2 x_2$	(2,1)

und damit

$$x_1 x_2^7 < x_1^2 x_2 < x_1^3 x_2^4 < x_1^3 x_2^5$$

Aufgabe 12.

1. Definieren Sie die Hilbertreihe eines graduierten Moduls.

Sei R eine graduierte K-Algebra und M ein graduierter R-Modul mit $\dim_K(M_i)$ endlich für alle $i \in \mathbb{Z}$. Dann heißt

$$H_M(t) := \sum_{i \in \mathbb{Z}} \dim_k(M_i)\, t^i$$

die Hilbert-Reihe von M.

2. Bestimmen Sie eine disjunkte Kegelzerlegung der vielfachenabgeschlossenen Teilmenge von $\mathrm{Mon}(\mathbb{C}[x_1, x_2])$, welche von $x_1^2 x_2^3$, x_2^4, und $x_1^3 x_2$ erzeugt wird.

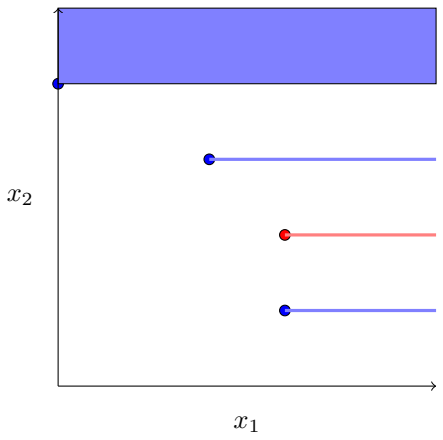

Abbildung 4: Disjunkte Kegelzerlegung.

Die disjunkte Kegelzerlegung kann aus Abbildung **??** abgelesen werden:

$$S\left(x_1^2 x_2^3, x_2^4, x_1^3 x_2\right) = x_1^3 x_2 \mathrm{Mon}(\mathbb{C}[x_1]) \uplus x_1^3 x_2^2 \mathrm{Mon}(\mathbb{C}[x_1]) \uplus x_1^2 x_2^3 \mathrm{Mon}(\mathbb{C}[x_1]) \uplus x_2^4 \mathrm{Mon}(\mathbb{C}[x_1, x_2])$$

3. Bestimmen Sie die Hilbertreihe der Menge aus (2).

Die (verallgemeinerte!) Hilbertreihe von S ist

$$H_S(t) = \frac{x_1^3 x_2 + x_1^3 x_2^2 + x_1^2 x_2^3}{1 - x_1} + \frac{x_2^4}{(1 - x_1)(1 - x_2)}$$

Aufgabe 13. Es sei $R = \mathbb{C}[x, y]$ und $J \trianglelefteq R$, das Ideal, welches von $f_1 := x^2 - y^2$, $f_2 := y^3 - 1$, und $f_3 := xy^3 - x$ erzeugt wird.

1. Zeigen Sie, dass $\{f_1, f_2, f_3\}$ mit multiplikativen Variablen (x, y), $(\bullet, y)$ und $(\bullet, y)$ eine Janetbasis von J bezüglich der lexikographischen Monomordnung (mit $x > y$) ist.

Zeige, dass $\{f_1, f_2, f_3\}$ vervollständigt und passiv ist.

Vervollständigt Eine Menge heißt vervollständigt, wenn die Leitmonome von $\{f_1, f_2, f_3\}$ die Kegelspitzen einer Zerlegung der Menge sind, die sie selbst erzeugen. Dies ist insbesondere dann der Fall, wenn die Menge passiv ist.

Passivitität Eine Menge heißt passiv, wenn die Leitmonome von $G := \{f_1, f_2, f_3\}$ die Kegelspitzen einer Zerlegung der Menge sind, die aus allen Leitmonomen von J sind. Zeige dazu

$$\forall g \in G\ \forall x \in \overline{M}(g) :\ N_G(xg) = 0$$

Es ist

$$\begin{array}{r} xf_2 = \underline{xy^3} - x \\ -f_3 = -\underline{xy^3} + x \\ \hline 0 \end{array}$$

und

$$\begin{array}{r} xf_3 = \underline{x^2y^3} - x^2 \\ -y^3 f_1 = -\underline{x^2y^3} + y^5 \\ \hline -\underline{x^2} + y^5 \\ f_1 = x^2 - y^2 \\ \hline \underline{y^5} - y^2 \\ -y^2 f_2 = -y^5 + y^2 \\ \hline 0 \end{array}$$

Somit ist die Menge passiv und vervollständigt und damit Janet-Basis.

2. Bestimmen Sie die verallgemeinerte Hilbertreihe von $S(J, <)$.

Es ist

$$H_{S(J,<)} = \frac{x^2}{(1 - x)(1 - y)} + \frac{y^3 + xy^3}{1 - y}$$

3. Bestimmen Sie $J \cap \mathbb{C}[y]$.

Da $<$ die Eliminationsordnung ist, gilt für eine Janet-Basis G von J, wie etwa G aus Aufgabenteil 1 eine ist:

$$J \cap \mathbb{C}[y] = \langle G \rangle \cap \mathbb{C}[y] = \langle G \cap \mathbb{C}[y] \rangle = \langle f_2 \rangle$$

Aufgabe 14.

1. Bestimmen Sie die Hilbertreihe des Invariantenrings $\mathbb{C}[x, y]^{\mathrm{D}_{10}}$ mit

$$\mathrm{D}_{10} := \left\langle \begin{pmatrix} \zeta_5 & 0 \\ 0 & \zeta_5^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \leq \mathrm{GL}_2(\mathbb{C})$$

Da $\mathrm{D}_{10} \leq \mathrm{GL}_2(\mathbb{C})$ endliche Gruppe und $R = \mathbb{C}[x,y]$ folgt mit dem Satz von Molien:

$$\begin{aligned} H_{R^G}(t) &:= \frac{1}{|G|} \sum_{g \in G} \det(1 - tg)^{-1} \\ &= \frac{1}{10} \sum_{i=0}^{4} \left(\det \begin{pmatrix} 1-\zeta_5^i t & 0 \\ 0 & 1-\zeta_5^{-i} t \end{pmatrix}^{-1} + \det \begin{pmatrix} 1 & -\zeta_5^i t \\ -\zeta_5^{-i} t & 1 \end{pmatrix}^{-1} \right) \\ &= \frac{1}{10} \left(\frac{5}{1-t^2} + \frac{1}{(1-t)^2} + 2 \sum_{i=1}^{2} \frac{1}{(1-\zeta_5^i)(1-\zeta_5^{-i})} \right) \end{aligned}$$

Aufgabe 15.

1. Definieren Sie den Begriff einer Ultrametrik.

Sei M Menge, $d : M \times M \to \mathbb{R}_{\geq 0}$. d heißt Ultrametrik, falls für alle $a, b, c \in M$ gilt:

1. $d(a,b) = 0 \iff a = b$,
2. $d(a,b) = d(b,a)$, und
3. $d(a,c) \leq \max(d(a,b), d(b,c))$.

(Vgl. Skript: Definition 4.3)

2. Zeigen Sie: Ist K ein bezüglich einer translationsinvarianten Ultrametrik vollständiger Körper und $(a_n)_{n\in\mathbb{N}}$ eine Folge in K, so gilt:

$$\left(\sum_{n=1}^{N} a_n \right)_{N \in \mathbb{N}} \text{ konvergent } \iff (a_n)_{n\in\mathbb{N}} \text{ ist Nullfolge.}$$

Sei $\left(\sum_{n=1}^{N} a_n \right)_{N \in \mathbb{N}}$ konvergent. Dann ist $\left(\sum_{n=1}^{N} a_n \right)_{N \in \mathbb{N}}$ insbesondere Cauchy-Folge, d.h.

$$\forall \epsilon > 0 \exists K \in \mathbb{N} \forall M, N \geq K : \; d\left(\sum_{n=1}^{N} a_n, \sum_{n=1}^{M} a_n \right) < \epsilon$$

Das gilt insbesondere für $M = N+1$. Dann folgt:

$$\forall \epsilon > 0 \exists K \in \mathbb{N} \forall N \geq K : \; d\left(\sum_{n=1}^{N} a_n, \sum_{n=1}^{N+1} a_n \right) < \epsilon \overset{\text{translationsinvariant}}{\Longrightarrow} d\left(0, \left(\sum_{n=1}^{N+1} a_n \right) - \left(\sum_{n=1}^{N} a_n \right) \right) = d(0, a_{N+1}) < \epsilon$$

Somit ist $(a_n)_{n\in\mathbb{N}}$ Nullfolge.

Für die Rückrichtung zeige, dass $\left(\sum_{n=1}^{N} a_n \right)_{N \in \mathbb{N}}$ Cauchy-Folge ist. Dazu

$$d\left(\sum_{n=M}^{N} a_n, 0 \right) \overset{\spadesuit}{=} d\left(\sum_{n=M+1}^{N} a_n, -a_M \right) \overset{\heartsuit}{\leq} \max\left\{ d\left(\sum_{n=M+1}^{N} a_n, 0 \right), d(-a_M, 0) \right\} \leq \ldots \leq \max\{ d(-a_n, 0) \mid M \leq n \leq N \}$$

Bei $\spadesuit$ wird ausgenutzt, dass d translationsinvariant ist. Bei $\heartsuit$ fließt ein, dass d Ultrametrik ist und somit die verschärfte Dreiecksungleichung gilt. $\max\{d(a_n,0) \mid M \leq n \leq N\}$ geht gegen Null, da $(a_n)_{n\in\mathbb{N}}$ Nullfolge ist. Somit ist $\left(\sum_{n=1}^{N} a_n \right)_{N \in \mathbb{N}}$ Cauchy-Folge und insbesondere konvergent.

3. Es sei (A,d) ein ultrametrischer Raum, $x \in A$ und $r \in \mathbb{R}_{>0}$. Zeigen Sie: Für alle $y \in B_r(x) := \{z \in A \mid d(x,z) < r\}$ gilt $B_r(y) = B_r(x)$.

Sei $y \in B_r(x)$ beliebig, d.h.

$$d(x,y) < r \tag{1}$$

Sei weiterhin $z \in B_r(y)$ beliebig, also

$$d(y,z) < r \tag{2}$$

Dann gilt:

$$d(z,x) \leq \max\left(\underbrace{d(z,y)}_{(??):<r}, \underbrace{d(y,x)}_{(??):<r}\right) < r$$

Sei umgekehrt $z' \in B_r(x)$ und folglich

$$d(x,z') < r \tag{3}$$

Dann gilt:

$$d(z',y) \leq \max\left(\underbrace{d(z,x)}_{(??):<r}, \underbrace{d(x,y)}_{(??):<r}\right) < r$$

Insgesamt folgt die Aussage. □

Aufgabe 16.

1. Formulieren Sie das Henselsche Lemma für das Liften von Nullstellen von Polynomen über vollständigen diskret bewerteten Körpern.

Sei K ein vollständiger Körper bezüglich der diskreten Bewertung ν mit Bewertungsring $R := R_\nu$. Weiter sei $f(t) \in R[t]$ ein Polynom und $a_0 \in R$ mit $\nu(f(a_0)) > 2\nu(f'(a_0))$. Dann gibt es ein $a_\infty \in R$ mit $f(a_\infty) = 0$. Genauer: Die durch $a_{i+1} := a_i - \frac{f(a_i)}{f'(a_i)}$ definierte Folge in R konvergiert gegen a_∞ mit $f(a_\infty) = 0$ und $\nu(a_\infty - a_0) \geq \nu(f(a_0)) - \nu(f'(a_0)) > 0$. (Vgl. Skript: Satz 4.19)

2. Bestimmen Sie alle $p \in \{5, 11, 13\}$, sodass ein $a \in \mathbb{Z}_p$ existiert mit $a^2 + a + 1 = 0$. Falls ein solches a existiert, so bestimmen Sie darüber hinaus ein $a_0 \in \mathbb{Z}$ mit $a_0 \equiv a \pmod{p^3}$.

$$f(a) = a^2 + a + 1$$

$p = 5$**:**

- $f(0) \equiv 1 \neq 0 \mod 5$,
- $f(1) \equiv 3 \neq 0 \mod 5$,
- $f(2) \equiv 2 \neq 0 \mod 5$,
- $f(3) \equiv 3 \neq 0 \mod 5$,
- $f(4) \equiv 1 \neq 0 \mod 5$.

$\implies$ keine Nullstelle in $\mathbb{F}_5$. $\implies$ keine Nullstelle in $\mathbb{Z}_5$.

$p = 11$**:**

- $f(0) \equiv 1 \neq 0 \mod 11$,
- $f(1) \equiv 3 \neq 0 \mod 11$,
- $f(2) \equiv 7 \neq 0 \mod 11$,
- $f(3) \equiv 2 \neq 0 \mod 11$,
- $f(4) \equiv 10 \neq 0 \mod 11$,
- $f(5) \equiv 9 \neq 0 \mod 11$,
- $f(6) \equiv 10 \neq 0 \mod 11$,
- $f(7) \equiv 2 \neq 0 \mod 11$,
- $f(8) \equiv 7 \neq 0 \mod 11$,
- $f(9) \equiv 3 \neq 0 \mod 11$,
- $f(10) \equiv 1 \neq 0 \mod 11$.

$\implies$ keine Nullstelle in $\mathbb{F}_{11}$. $\implies$ keine Nullstelle in $\mathbb{Z}_{11}$.

$p = 11$**:**

- $f(0) \equiv 1 \neq 0 \mod 13$,
- $f(1) \equiv 3 \neq 0 \mod 13$,
- $f(2) \equiv 7 \neq 0 \mod 13$,
- $f(3) = 13 \equiv 0 \neq 0 \mod 13$.

$\Longrightarrow$ $a_0 = 3$ Kandidat für Nullstelle. Es gilt $f'(a) = 2a + 1$. Weiter ist $f'(3) = 7$. Damit gilt

$$\nu_{13}(f(b_0)) = \nu_{13}(13) = 1 > 0 = 2\nu_{13}(7) = 2\nu_{13}(f'(b_0))$$

$\Longrightarrow$ $\exists a \in \mathbb{Z}_{13} : a^2 + a + 1 = 0$. Weiterhin gilt mit

$$d := \nu_{13}(f(b_0)) - 2\nu_{13}(f'(b_0)) = 1$$

für die durch

$$b_{n+1} := b_n - \frac{f(b_n)}{f'(b_n)} = b_n - \frac{b_n^2 + b_n + 1}{2b_n + 1} = \frac{b_n(2b_n + 1) - \left(b_n^2 + b_n + 1\right)}{2b_n + 1} = \frac{2b_n^2 + b_n - b_n^2 - b_n - 1}{2b_n + 1} = \frac{b_n^2 - 1}{2b_n + 1}$$

rekursiv definierte Folge

$$\nu(b_n - a) \geq (2^n - 1)\, d + \nu(f'(b_0)) = 2^n - 1$$

Für eine Genauigkeit modulo p^3 muss also b_2 berechnet werden. Es gilt:

$$b_1 := \frac{b_0^2 - 1}{2b_0 + 1} = \frac{3^2 - 1}{2 \cdot 3 + 1} = \frac{8}{7}$$
$$b_2 := \frac{b_1^2 - 1}{2b_1 + 1} = \frac{\left(\frac{8}{7}\right)^2 - 1}{2\left(\frac{8}{7}\right) + 1} = \frac{\frac{64-49}{49}}{\frac{16+7}{7}} = \frac{15 \cdot 7}{49 \cdot 23} = \frac{15}{7 \cdot 23} = \frac{15}{161}$$

Es gilt also

$$a \equiv \frac{15}{161} \mod 13^3$$

Um nun eine Lösung in $\mathbb{Z}$ zu erhalten, kann man die p-adische Entwicklung von $b_2 = \frac{15}{161}$ betrachten:

$$\frac{15}{161} = 15 \cdot \frac{1}{161}$$

Weiter gilt $15 = (2, 1)_{13}$ und $161 = (5, -1, 1)_{13}$. Man bestimme nun $161^{-1} \mod 13^3$. Nach einiger Rechnung ergibt sich:

$$\frac{15}{161} \equiv (2,1)_{13} \cdot (-5, 2, -4, 1)_{13} = (3, -6)_{13} + (0, 4, 2)_{13} + (0, 0, 5, -5)_{13} + (0, 0, 0, 2, 1)_{13} = (3, -2, -6, -2, -1)_{13} \mod 13^3$$

Um mod p^3 übereinzustimmen muss man mindestens die ersten drei Stellen übernehmen:

$$a_0 = 3 \cdot 13^0 + (-2) \cdot 13^1 + (-6) \cdot 13^2 = -1037$$