M. Künzer

Galoistheorie, WS 08/09

Lösung 1

Aufgabe 1

(1) Die Substitution liefert

$$\begin{aligned} x^3 + ax^2 + bx + c &= (y - \tfrac{a}{3})^3 + a(y - \tfrac{a}{3})^2 + b(y - \tfrac{a}{3}) + c \\ &= y^3 + (b - \tfrac{1}{3}a^2)y + (\tfrac{2}{27}a^3 - \tfrac{1}{3}ab + c)\ . \end{aligned}$$

Also wird $p = b - \frac{1}{3}a^2$ und $q = \frac{2}{27}a^3 - \frac{1}{3}ab + c$.

(2) Die Substitution liefert für $z \neq 0$

$$\begin{aligned} y^3 + py + q &= (z - \tfrac{p}{3z})^3 + p(z - \tfrac{p}{3z}) + q \\ &= z^3 + q - \tfrac{p^3}{27}z^{-3}\ . \end{aligned}$$

Mit $y = z - \frac{p}{3z}$ ist also $z^3 + q - \frac{p^3}{27}\, z^{-3} = y^3 + py + q$ für $z \neq 0$. Finden wir ein $z \in \mathbf{C} \setminus \{0\}$, das Nullstelle der linken Seite ist, so ist das zugehörige y Nullstelle der rechten Seite.

(3) Beachte, daß für $z \in \mathbf{C}$ mit $(z^3)^2 + qz^3 - \frac{p^3}{27} = 0$ wegen $p \neq 0$ auch $z \neq 0$ ist. Also ist

$$\begin{aligned} \{z \in \mathbf{C} \setminus \{0\} \ :\ z^3 + q - \tfrac{p^3}{27}z^{-3} = 0\} &= \{z \in \mathbf{C} \ :\ (z^3)^2 + qz^3 - \tfrac{p^3}{27} = 0\} \\ &= \left\{z \in \mathbf{C} \ :\ z^3 = -\tfrac{q}{2} \pm \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}\right\}\ . \end{aligned}$$

Beachte, daß die letzte Gleichung im Komplexen im Falle + und im Falle − im allgemeinen je 3 Lösungen hat. In der Tat, ist $w = |w| \exp(\mathrm{i} \arg w) \in \mathbf{C} \setminus \{0\}$, so ist $z = \sqrt[3]{|w|} \exp(\mathrm{i} \arg w/3 + 2\pi \mathrm{i} k/3)$ eine Lösung von $z^3 = w$ für $k \in \{0, 1, 2\}$

(4) Die Substitution in (1) liefert $p = \frac{5}{12}$ und $q = -\frac{31}{54}$. Wir haben also gemäß (2)

$$z^6 - \tfrac{31}{54}z^3 + \tfrac{125}{46656} \ = \ 0$$

zu lösen. Nun ist $\sqrt{\frac{1}{4}(-\frac{31}{54})^2 - \frac{125}{46656}} = \frac{7}{24}$. Also können wir etwa

$$z^3 \ = \ -\tfrac{1}{2} \cdot (-\tfrac{31}{54}) + \tfrac{7}{24} \ = \ \tfrac{125}{216}$$

ansetzen (Fall + in (3)) und $z = \sqrt[3]{\frac{125}{216}} = \frac{5}{6}$ verwenden.

Somit wird $y = z - \frac{1}{3} \cdot \frac{5}{12}\, z^{-1} = \frac{2}{3}$.

Schließlich wird $x = y - \frac{1}{3} \cdot \frac{1}{2} = \frac{1}{2}$ eine Lösung von $x^3 + \frac{1}{2}x^2 + \frac{1}{2}x - \frac{1}{2} = 0$.

(Die komplette Faktorisierung ergibt sich zu

$$x^3 + \tfrac{1}{2}x^2 + \tfrac{1}{2}x - \tfrac{1}{2} \ = \ (x - \tfrac{1}{2})(x + \tfrac{1}{2} - \tfrac{\mathrm{i}}{2}\sqrt{3})(x + \tfrac{1}{2} + \tfrac{\mathrm{i}}{2}\sqrt{3})\ .\ )$$

Der Fall dreier verschiedener reeller Nullstellen (casus irreducibilis) eines Polynoms dritten Grades mit reellen Koeffizienten ist mit diesem Verfahren haarig, da man selbst bei ganzzahligen Nullstellen diese nicht immer aus den erhaltenen verschachtelten Wurzelausdrücken komplexer Zahlen erkennen kann. Aber immerhin finden wir eine Lösung, wenn auch manchmal nicht in optimaler Gestalt.

Aufgabe 2

(1) Eine positive ganze Zahl teilt a und b genau dann, wenn sie $\mathrm{ggT}(a,b)$ teilt. Diese Eigenschaft legt $\mathrm{ggT}(a,b)$ auch fest, da eine positive ganze Zahl durch die Menge ihrer Teiler bestimmt ist – als deren Maximum.

Wir haben also zu zeigen, daß $x \in \mathbf{Z}_{\geqslant 0}$ genau dann a und b teilt, wenn sie a und r teilt.

Teile x die beiden Zahlen a und b. Dann ist x auch ein Teiler von $b - aq = r$.

Teile umgekehrt x die beiden Zahlen a und r. Dann ist x auch ein Teiler von $aq + r = b$.

(2) Es ist $x_0 > x_1 > x_2 > \dots$ eine strikt fallende Folge nichtnegativer ganzer Zahlen. Diese muß an einer Stelle Null werden, was die Existenz von ℓ mit $x_\ell > 0$ und $x_{\ell+1} = 0$ zeigt.

Desweiteren ist mit (1)

$$\mathrm{ggT}(a,b) \;=\; \mathrm{ggT}(x_0,x_1) \;=\; \mathrm{ggT}(x_1,x_2) \;=\; \cdots \;=\; \mathrm{ggT}(x_\ell,x_{\ell+1}) \;=\; \mathrm{ggT}(x_\ell,0) \;=\; x_\ell\ .$$

(3) Wir behaupten, daß $x_k s_k + x_{k-1} s_{k+1} = x_\ell$ für alle $k \in [1,\ell]$, insbesondere also für $k = 1$. Wir führen eine absteigende Induktion nach k. Der Induktionsanfang ist durch $x_\ell s_\ell + x_{\ell-1} s_{\ell+1} = x_\ell$ gesichert. Für den Induktionsschritt nehmen wir $x_k s_k + x_{k-1} s_{k+1} = x_\ell$ für ein $k \in [2,\ell]$ als bekannt an. Wir erhalten

$$\begin{aligned} x_{k-1}s_{k-1} + x_{k-2}s_k &= x_{k-1}(s_{k+1} - s_k q_{k-1}) + (x_{k-1}q_{k-1} + x_k)s_k \\ &= x_k s_k + x_{k-1} s_{k+1} \\ &= x_\ell\ . \end{aligned}$$

(4) Euklid liefert

$$\begin{aligned} 87 &= 23 \cdot 3 + 18 \\ 23 &= 18 \cdot 1 + 5 \\ 18 &= 5 \cdot 3 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0\ . \end{aligned}$$

Hier bricht der Algorithmus wegen des erhaltenen Restes 0 ab. Also ist $x_0 = 87$, $x_1 = 23$, $x_2 = 18$, $x_3 = 5$, $x_4 = 3$, $x_5 = 2$, $x_6 = 1$ und $x_7 = 0$. Insbesondere ist $\ell = 6$. Ferner werden $q_1 = 3$, $q_2 = 1$, $q_3 = 3$, $q_4 = 1$, $q_5 = 1$ und $q_6 = 2$.

Es folgt $\mathrm{ggT}(23,87) = 1$.

> Dies hätte man auch mit Primfaktorzerlegungen erkennen können. Bei großen Zahlen ist eine solche Zerlegung allerdings schwieriger durchzuführen als der Euklidsche Algorithmus.

Darüberhinaus erhalten wir als Folge der s_k mittels $s_{k-1} = s_{k+1} - s_k q_{k-1}$ folgendes, angefangen mit $s_7 = 0$, $s_6 = 1$.

$$\begin{aligned} s_5 &= 0 - 1 \cdot 1 &&= -1 \\ s_4 &= 1 - (-1) \cdot 1 &&= 2 \\ s_3 &= (-1) - 2 \cdot 3 &&= -7 \\ s_2 &= 2 - (-7) \cdot 1 &&= 9 \\ s_1 &= (-7) - 9 \cdot 3 &&= -34 \end{aligned}$$

Also wird $1 = x_\ell = x_1 s_1 + x_0 s_2 = 23 \cdot (-34) + 87 \cdot 9$, wie man leicht durch Nachrechnen nochmals bestätigt.

Aufgabe 3

(1) Es ist $4 \cdot 3 + 1 \equiv_7 13 \equiv_7 -1$.

> Gemäß unserer Konvention wäre es auch zulässig gewesen, $4 \cdot 3 + 1 = -1$ zu schreiben, da aus dem Kontext hervorgeht, daß wir in $\mathbf{Z}/7\mathbf{Z}$ rechnen.

Es ist $6 \cdot 5 \cdot 4 = 30 \cdot 4 \equiv_7 2 \cdot 4 \equiv_7 1$.

(2) Es ist $3 \cdot 5 \cdot 7 \cdot 9 = 15 \cdot 63 \equiv_{32} 15 \cdot (-1) = -15$.

Es ist $31^{31} \equiv_3 2(-1)^{31} \equiv_{32} -1$.

Es ist $4^3 = 64 \equiv_{32} 0$.

Aufgabe 4

(1) Sei $g := \mathrm{ggT}(k, m) > 1$. *Nehmen wir an,* es ist $k + m\mathbf{Z}$ invertierbar. Dann gibt es ein $\ell \in \mathbf{Z}$ mit $k\ell \equiv_m 1$. Somit gibt es ein $u \in \mathbf{Z}$ mit $k\ell + um = 1$. Da aber g sowohl k als auch m teilt, teilt g auch $k\ell + um = 1$, *Widerspruch.*

Sei $\mathrm{ggT}(k, m) = 1$. Mit dem Euklidschen Algorithmus aus Aufgabe 2.(3) gibt es $s, t \in \mathbf{Z}$ mit $sk + tm = 1$. Also ist $sk \equiv_m 1$, d.h. $(s + m\mathbf{Z})(k + m\mathbf{Z}) = 1 + m\mathbf{Z}$.

Es ist $23 \cdot (-34) + 87 \cdot 9 = 1$, vgl. Aufgabe 2.(4). Also ist $23 \cdot (-34) \equiv_{87} 1$, d.h. $(23 + 87\mathbf{Z})^{-1} = -34 + 87\mathbf{Z}$.

Um $(17 + 1000\mathbf{Z})^{-1}$ zu berechnen, verwenden wir ebenfalls den Euklidschen Algorithmus. Wir erhalten

$$\begin{aligned} 1000 &= 17 \cdot 58 + 14 \\ 17 &= 14 \cdot 1 + 3 \\ 14 &= 3 \cdot 4 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0\,, \end{aligned}$$

wobei uns $\mathrm{ggT}(1000, 17) = 1$ gar nicht so sehr interessiert, sondern vielmehr

$$\begin{aligned} 0 - 1 \cdot 1 &= -1 \\ 1 - (-1) \cdot 4 &= 5 \\ (-1) - 5 \cdot 1 &= -6 \\ 5 - (-6) \cdot 58 &= 353\,, \end{aligned}$$

und also $353 \cdot 17 + (-6) \cdot 1000 = \mathrm{ggT}(1000, 17) = 1$.

(2) Ist $1/n = 0.\overline{a_1 a_2 \ldots a_k}$ mit Ziffern $a_i \in [0, 9]$, so bedeutet dies, daß $\frac{a_1 a_2 \ldots a_k}{99\ldots9} = 1/n$ (k-mal die Ziffer 9), und $k \geqslant 1$ ist minimal so gewählt, daß dies möglich ist. In anderen Worten, $k \geqslant 1$ ist minimal so gewählt, daß n ein Teiler von $10^k - 1$ ist. Abermals in anderen Worten, $k \geqslant 1$ ist minimal so gewählt, daß $10^k \equiv_n 1$.

Es ist $1/7 = 0.\overline{142857}$, die Periodenlänge ist also gleich 6. Und in der Tat ist

$$\begin{aligned} 10^1 &\equiv_7 3 \equiv_7 3 \\ 10^2 &\equiv_7 30 \equiv_7 2 \\ 10^3 &\equiv_7 20 \equiv_7 -1 \\ 10^4 &\equiv_7 -10 \equiv_7 -3 \\ 10^5 &\equiv_7 -30 \equiv_7 -2 \\ 10^6 &\equiv_7 -20 \equiv_7 1\,. \end{aligned}$$

Es ist $1/41 = 0.\overline{02439}$, die Periodenlänge ist also gleich 5. Und in der Tat ist

$$\begin{aligned} 10^1 &\equiv_{41} 10 \equiv_{41} 10 \\ 10^2 &\equiv_{41} 100 \equiv_{41} 18 \\ 10^3 &\equiv_{41} 180 \equiv_{41} 16 \\ 10^4 &\equiv_{41} 160 \equiv_{41} -4 \\ 10^5 &\equiv_{41} -40 \equiv_{41} 1\,. \end{aligned}$$