M. Künzer

Galoistheorie, WS 08/09

Lösung 2

Aufgabe 5

(1) Die Substitution liefert

$$\begin{array}{rcl} x^4 + ax^3 + bx^2 + cx & = & (y - \frac{a}{4})^4 + a(y - \frac{a}{4})^3 + b(y - \frac{a}{4})^2 + c(y - \frac{a}{4}) + d \\ & = & y^4 + (b - \frac{3}{8}a^2)y^2 + (\frac{1}{8}a^3 - \frac{1}{2}ab + c)y + (\frac{1}{16}a^2b - \frac{3}{256}a^4 - \frac{1}{4}ac + d) \end{array}$$

Also wird $p = b - \frac{3}{8}a^2$, $q = \frac{1}{8}a^3 - \frac{1}{2}ab + c$ und $r = \frac{1}{16}a^2b - \frac{3}{256}a^4 - \frac{1}{4}ac + d$.

(2) Zunächst können wir in beiden Fällen die Gleichung $y^4 + py^2 + qy + r = 0$ für noch beliebiges $\alpha \in \mathbf{C}$ äquivalent umformen zu

$$(*) \qquad (y^2 - \alpha)^2 \;=\; -(2\alpha + p)y^2 - qy + (\alpha^2 - r)\ .$$

Sei nun $\alpha \in \mathbf{C}$ so gewählt, daß $\alpha^3 + \frac{1}{2}p\alpha^2 - r\alpha - \frac{1}{2}pr + \frac{1}{8}q^2 = 0$.

Ist $p + 2\alpha = 0$, so kann nach Wahl von α nur $q = 0$ gewesen sein. Dann aber schreibt sich die Gleichung $(*)$

$$(y^2 - \alpha)^2 \;=\; \alpha^2 - r\ .$$

Ist $p + 2\alpha \neq 0$, dann wird

$$\begin{array}{rcl} -(2\alpha + p)(y + \frac{q}{2(2\alpha+p)})^2 & = & -(2\alpha + p)y^2 - qy - \frac{q^2}{4(2\alpha+p)} \\ & = & -(2\alpha + p)y^2 - qy + \frac{2\alpha^3 + p\alpha^2 - 2r\alpha - pr}{2\alpha+p} \\ & = & -(2\alpha + p)y^2 - qy + \frac{(2\alpha+p)(\alpha^2 - r)}{2\alpha+p} \\ & = & -(2\alpha + p)y^2 - qy + (\alpha^2 - r)\ . \end{array}$$

Die Bedingung an α ergibt sich aus der Forderung, die Diskriminante der rechten Seite von $(*)$, gesehen als quadratisches Polynom in y, verschwinden zu lassen.

(3) Die Substitution in (1) liefert $p = 1$, $q = \gamma$ und $r = -\frac{1}{2}$.

Ein $\alpha \in \mathbf{C}$, welches die Gleichung $\alpha^3 + \frac{1}{2}\alpha^2 + \frac{1}{2}\alpha - \frac{1}{2} = 0$ erfüllt, ist nach Aufgabe 1.(4) z.B. mit $\alpha = \frac{1}{2}$ gegeben. Da $p + 2\alpha = 2 \neq 0$, haben wir ein $y \in \mathbf{C}$ mit

$$(y^2 - \tfrac{1}{2})^2 \;=\; -2(y + \tfrac{\gamma}{4})^2\ .$$

zu finden. Hierfür lösen wir etwa

$$y^2 - \tfrac{1}{2} \;=\; \mathrm{i}\sqrt{2}(y + \tfrac{\gamma}{4})$$

(wofür wir auch das Negative der rechten Seite hätten heranziehen können). Wir formen nach Einsetzen des Wertes von γ äquivalent um zu

$$y^2 - \mathrm{i}\sqrt{2}\cdot y + \tfrac{1}{2}(\sqrt{3} - 1) \;=\; 0$$

Wir erhalten etwa

$$y \;=\; \mathrm{i}\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt[4]{3}}{\sqrt{2}}\ ,$$

und also

$$x \;=\; -1 + \mathrm{i}\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt[4]{3}}{\sqrt{2}}\ .$$

(Die vollständige Faktorisierung lautet

$$x^4 + 4x^3 + 7x^2 + (6 + \gamma)x + \tfrac{3}{2} + \gamma \;=\;$$
$$(x + 1 - \mathrm{i}\tfrac{\sqrt{2}}{2} - \mathrm{i}\tfrac{\sqrt[4]{3}}{\sqrt{2}})(x + 1 - \mathrm{i}\tfrac{\sqrt{2}}{2} + \mathrm{i}\tfrac{\sqrt[4]{3}}{\sqrt{2}})(x + 1 + \mathrm{i}\tfrac{\sqrt{2}}{2} - \tfrac{\sqrt[4]{3}}{\sqrt{2}})(x + 1 + \mathrm{i}\tfrac{\sqrt{2}}{2} + \tfrac{\sqrt[4]{3}}{\sqrt{2}})\ .)$$

Aufgabe 6

(1) Setze an mit $0 = 0_{R\times S} := (0_R, 0_S)$ und $1 = 1_{R\times S} := (1_R, 1_S)$. Setze an mit $-(r,s) := (-r,-s)$ für $r \in R$ und $s \in S$..

Für (r,s), (r',s'), $(r'',s'') \in R \times S$ wird

$$\begin{array}{lcl cl}
(r,s)+(r',s') & = & (r+r',s+s') & = & (r'+r,s'+s) \\
 & & & = & (r',s')+(r,s) \\
(r,s)+(0,0) & = & (r+0,s+0) & = & (r,s) \\
(r,s)+(-r,-s) & = & (r-r,s-s) & = & (0,0) \\
((r,s)+(r',s'))+(r'',s'') & = & ((r+r')+r'',(s+s')+s'') & = & (r+(r'+r''),s+(s'+s'')) \\
 & & & = & (r,s)+((r',s')+(r''+s'')) \\
(r,s)\cdot(r',s') & = & (r\cdot r',s\cdot s') & = & (r'\cdot r,s'\cdot s) \\
 & & & = & (r',s')\cdot(r,s) \\
(r,s)\cdot(1,1) & = & (r\cdot 1,s\cdot 1) & = & (r,s) \\
((r,s)\cdot(r',s'))\cdot(r'',s'') & = & ((r\cdot r')\cdot r'',(s\cdot s')\cdot s'') & = & (r\cdot(r'\cdot r''),s\cdot(s'\cdot s'')) \\
 & & & = & (r,s)\cdot((r',s')\cdot(r''\cdot s'')) \\
((r,s)+(r',s'))\cdot(r'',s'') & = & ((r+r')\cdot r'',(s+s')\cdot s'') & = & (r\cdot r''+r'\cdot r'',s\cdot s''+s'\cdot s'') \\
 & & & = & (r,s)\cdot(r'',s'')+(r',s')\cdot(r'',s'')\ .
\end{array}$$

Kurz, die Ringeigenschaften sind erfüllt, da sie eintragsweise erfüllt sind.

Sind R und S Körper, so sind zwar $(1,0)$ und $(0,1)$ ungleich $(0,0)$, aber $(1,0)(0,1) = (0,0)$. Also ist $R \times S$ diesenfalls kein Körper. (Es ist noch nicht einmal ein Integritätsbereich.)

(2) Die Abbildung

$$\begin{array}{ccccc}
R & \longrightarrow & R/I & \times & R/J \\
r & \longmapsto & (r+I & , & r+J)
\end{array}$$

ist ein Ringmorphismus, da 1 auf $1 = (1+I, 1+J)$ abgebildet wird, da die Summe $r+s$ auf $(r+s+I, r+s+J) = (r+I, r+J) + (s+I, s+J)$ abgebildet wird und da für $r,\ s \in R$ das Produkt $r \cdot s$ auf $(r\cdot s+I, r\cdot s+J) = (r+I,r+J)\cdot(s+I,s+J)$ abgebildet wird, wobei $r,\ s \in R$.

Dieser hat Kern $I\cap J$, da ein Element r genau dann auf 0 abgebildet wird, wenn $r+I = 0+I$ und $r+J = 0+J$, d.h. genau dann, wenn $r \in I\cap J$. Das Lemma aus §1.4.3 gibt den injektiven Ringmorphismus

$$\begin{array}{ccccc}
R/(I\cap J) & \longrightarrow & R/I & \times & R/J \\
r+(I\cap J) & \longmapsto & (r+I & , & r+J)\ .
\end{array}$$

Wir haben die Surjektivität dieses Ringmorphismus zu zeigen. Nun ist nach Voraussetzung $I+J = R$, wir können also $x \in I$ und $y \in J$ mit $x+y = 1$ finden. Es wird

$$x+I\cap J \longmapsto (x+I,x+J) \ = \ (0+I,x+y+J) \ = \ (0+I,1+J)$$

abgebildet. Ferner wird

$$y+I\cap J \longmapsto (y+I,y+J) \ = \ (y+x+I,0+J) \ = \ (1+I,0+J)$$

abgebildet.

Sei nun $(u+I, v+J) \in R/I \times R/J$ vorgegeben. Da ein Ringmorphismus vorliegt, wird in der Tat

$$\begin{array}{rcl}
uy+vx+I\cap J & \longmapsto & (u+I,u+J)(y+I,y+J)+(v+I,v+J)(x+I,x+J) \\
 & = & (u+I,u+J)(1+I,0+J)+(v+I,v+J)(0+I,1+J) \\
 & = & (u+I,0+J)+(0+I,v+J) \\
 & = & (u+I,v+J)\ .
\end{array}$$

Kurz, da y auf $(1,0)$ und x auf $(0,1)$ geht, müssen nur y und x entsprechend zusammengesetzt werden, um im Bild $(r+I, s+J)$ zu erhalten.

Wir merken uns noch für Verwendung in (3), daß $uy + vx + I \cap J$ ein Urbild, und wegen Injektivität das Urbild von $(u+I, v+J)$ ist.

(3) Mit (2) bleibt zum einen zu zeigen, daß $m\mathbf{Z} + n\mathbf{Z} = \mathbf{Z}$, i.e. daß $m\mathbf{Z} + n\mathbf{Z} \supseteq \mathbf{Z}$. Da aber $1 = ms + nt \in m\mathbf{Z} + n\mathbf{Z}$ ist, ist auch $\mathbf{Z} = 1\mathbf{Z} \subseteq m\mathbf{Z} + n\mathbf{Z}$.

Zum anderen müssen wir $m\mathbf{Z} \cap n\mathbf{Z} = mn\mathbf{Z}$ nachweisen. Die Inklusion $\supseteq$ ist ersichtlich, auch ohne Verwendung der Voraussetzung $\mathrm{ggT}(m,n) = 1$.

Zeigen wir die Inklusion $\subseteq$. Sei $x \in m\mathbf{Z} \cap n\mathbf{Z}$. Schreibe $x = ma = nb$ für gewisse $a,\, b \in \mathbf{Z}$. Insbesondere teilt n das Produkt ma. Da n und m teilerfremd sind, teilt n daher a. Wir schreiben $a = nc$ für ein $c \in \mathbf{Z}$. Es wird $x = ma = mnc \in mn\mathbf{Z}$.

Der Isomorphismus in die eine Richtung ist wie in (2) gegeben durch

$$\begin{array}{rcccc} \mathbf{Z}/mn\mathbf{Z} & \xrightarrow{\sim} & \mathbf{Z}/m\mathbf{Z} & \times & \mathbf{Z}/n\mathbf{Z} \\ z + mn\mathbf{Z} & \longmapsto & (z + m\mathbf{Z} & , & z + n\mathbf{Z})\ . \end{array}$$

Da $ms + nt = 1$, folgt mit der Bemerkung am Ende von (2), daß für $u,\, v \in \mathbf{Z}$ das Urbild eines Elements $(u + m\mathbf{Z}, v + n\mathbf{Z})$ der rechten Seite durch $unt + vms + mn\mathbf{Z}$ gegeben ist. Dies liefert die Umkehrbijektion

$$\begin{array}{rcccc} \mathbf{Z}/mn\mathbf{Z} & \xleftarrow{\sim} & \mathbf{Z}/m\mathbf{Z} & \times & \mathbf{Z}/n\mathbf{Z} \\ unt + vms + mn\mathbf{Z} & \longleftarrow\!\!| & (u + m\mathbf{Z} & , & v + n\mathbf{Z})\ . \end{array}$$

Nach der ersten Bemerkung in §1.4.1 ist die Umkehrbijektion eines Ringisomorphismus ebenfalls ein Ringisomorphismus. (Dies hier direkt zu prüfen, wäre etwas lästig!)

(4) Die Aussage über den Isomorphismus folgt wegen $\mathrm{ggT}(3,4) = 1$ aus (3).

Finden wir nun die Isomorphismen in beide Richtungen. Es ist $3 \cdot (-1) + 4 \cdot 1 = 1$, wie man auch ohne Euklid erkennt. Wir haben also $m = 3$, $s = -1$, $n = 4$ und $t = 1$ in die Lösung von (3) einzusetzen. Wir erhalten so

$$\begin{array}{rcccc} \mathbf{Z}/12\mathbf{Z} & \xrightarrow{\sim} & \mathbf{Z}/3\mathbf{Z} & \times & \mathbf{Z}/4\mathbf{Z} \\ z + 12\mathbf{Z} & \longmapsto & (z + 3\mathbf{Z} & , & z + 4\mathbf{Z})\ . \end{array}$$

in die eine und

$$\begin{array}{rcccc} \mathbf{Z}/12\mathbf{Z} & \xleftarrow{\sim} & \mathbf{Z}/3\mathbf{Z} & \times & \mathbf{Z}/4\mathbf{Z} \\ 4u - 3v + 12\mathbf{Z} & \longleftarrow\!\!| & (u + 3\mathbf{Z} & , & v + 4\mathbf{Z})\ . \end{array}$$

in die andere Richtung.

(Elementar ausgedrückt bedeutet dies nun, daß bei gegebenen $u,\, v \in \mathbf{Z}$ die Lösungen des Kongruenzsystems

$$\begin{array}{ccc} x & \equiv_3 & u \\ x & \equiv_4 & v \end{array}$$

gegeben sind durch $x \in \{4u - 3v + 12k \ :\ k \in \mathbf{Z}\}$.)