M. Künzer

Galoistheorie, WS 08/09

Lösung 3

Aufgabe 7

(1) Um zu zeigen, daß $K \xrightarrow{f} R$ injektiv ist, müssen wir gemäß Lemma in §1.4.3 zeigen, daß $\operatorname{Kern} f = \{0_K\}$.

Mit demselben Lemma wissen wir, daß $\operatorname{Kern} f \subseteq K$ ein Ideal ist. Dank der letzten Bemerkung aus §1.2 wissen wir, daß dies $\operatorname{Kern} f = \{0_K\}$ oder $\operatorname{Kern} f = K$ zur Folge hat.

Sei *angenommen,* es ist $\operatorname{Kern} f = K$. Dann bildet f alle Elemente von K auf 0_R ab. Insbesondere wird $1_R = f(1_K) = 0_R$. Ist nun $x \in R$, so wird $x = x \cdot 1_R = x \cdot 0_R = 0_R$, und mithin $R = \{0_R\}$, *Widerspruch.*

Also ist $\operatorname{Kern} f = \{0_K\}$, wie zu zeigen war.

(2) Es ist $\varphi : K[X] \longrightarrow K,\ f(X) \longmapsto f(0) = f_0$ ein Ringmorphismus, wie man entweder direkt verifiziert, oder aber aus der Bemerkung aus §1.6.2 mit $n = 1$, $a = \mathrm{id}_K$ und $s = 0$ entnimmt – kurz, die Prozedur des Einsetzens der 0 ist ein Ringmorphismus.

Ist $f(X) = \sum_{i \geqslant 0} f_i X^i \in \operatorname{Kern} \varphi$, so ist $f_0 = 0$, und wir können $f(X) = X \cdot (\sum_{i \geqslant 1} f_{i+1} X^i)$ schreiben. Somit ist $\operatorname{Kern} \varphi \subseteq XR[X]$.

Ist umgekehrt $f(X) \in XR[X]$, so können wir $f(X) = Xg(X)$ für ein $g(X) \in R[X]$ schreiben und erhalten durch Koeffizientenvergleich $f_0 = 0$.

Insgesamt ist also $\operatorname{Kern} \varphi = XR[X]$.

Das Lemma aus §1.4.3 zeigt nun, da φ surjektiv ist, daß $R[X]/\operatorname{Kern} \varphi \simeq R$ ist.

Aufgabe 8

(1) Es ist $h(X) = f(X)q(X) + r(X)$. Wir haben zu zeigen, daß

$$f(X)K[X] + h(X)K[X] \overset{!}{=} f(X)K[X] + r(X)K[X]\,.$$

Da $h(X) = f(X)q(X) + r(X)$, ist $h(X)$ in der rechten Seite enthalten. Da auch $f(X)$ in der rechten Seite enthalten ist, ist jedes Element der linken Seite in der rechten Seite enthalten.

Da $r(X) = -f(X)q(X) + h(X)$, ist $r(X)$ in der linken Seite enthalten. Da auch $f(X)$ in der linken Seite enthalten ist, ist jedes Element der rechten Seite in der linken Seite enthalten.

(2) Es ist $\deg u_1 > \deg u_2 > \deg u_3 > \ldots$ strikt fallend und kann daher nicht unendlich lang in $\mathbf{Z}_{\geqslant 0}$ fortgesetzt werden. Also muß es ein $\ell \geqslant 0$ geben, bei dem zwar noch $\deg u_\ell \geqslant 0$, aber $\deg u_{\ell+1} = -\infty$ ist, i.e. $u_{\ell+1}(X) = 0$.

Mit (1) ist nun

$$\begin{array}{rcl} h(X)K[X] + f(X)K[X] & = & u_0(X)K[X] + u_1(X)K[X] \\ & = & u_1(X)K[X] + u_2(X)K[X] \\ & = & \cdots \\ & = & u_\ell(X)K[X] + u_{\ell+1}(X)K[X] \\ & = & g(X)K[X] + 0 \cdot K[X] \\ & = & g(X)K[X]\,. \end{array}$$

(3) Wir behaupten, daß $u_k(X)s_k(X) + u_{k-1}(X)s_{k+1}(X) = g(X)$ für alle $k \in [1, \ell]$, insbesondere also für $k = 1$, was dann $f(X)s_1(X) + h(X)s_2(X) = g(X)$ gibt.

Wir führen eine absteigende Induktion nach k. Der Induktionsanfang ist durch $u_\ell(X)s_\ell(X) + u_{\ell-1}(X)s_{\ell+1}(X) = u_\ell(X) = g(X)$ gesichert. Für den Induktionsschritt nehmen wir $u_k(X)s_k(X) + u_{k-1}(X)s_{k+1}(X) = g(X)$ für ein $k \in [2, \ell]$ als bekannt an. Wir erhalten

$$\begin{array}{rl} & u_{k-1}(X)s_{k-1}(X) + u_{k-2}(X)s_k(X) \\ = & u_{k-1}(X)(s_{k+1}(X) - s_k(X)q_{k-1}(X)) + (u_{k-1}(X)q_{k-1}(X) + u_k(X))s_k(X) \\ = & u_{k-1}(X)s_{k+1}(X) + u_k(X)s_k(X) \\ = & g(X)\ . \end{array}$$

(4) Euklid liefert

$$\begin{array}{lcl} (X^8 + X^3 + X + 1) & = & (X^3 + 1)(X^5 + X^2 + 1) + (X^2 + X) \\ (X^3 + 1) & = & (X^2 + X)(X + 1) + (X + 1) \\ (X^2 + X) & = & (X + 1)X + 0\ . \end{array}$$

Also ist $\ell = 3$ und $g(X) = X + 1$, und wir erhalten als Folge der $s_k(X)$ mit $s_4(X) = 0$ und $s_3(X) = 1$

$$\begin{array}{rclcl} s_2(X) & = & 0 - 1 \cdot (X + 1) & = & X + 1 \\ s_1(X) & = & 1 - (X + 1) \cdot (X^5 + X^2 + 1) & = & X^6 + X^5 + X^3 + X^2 + X \end{array}$$

Es wird so $f(X)s_1(X) + h(X)s_2(X) = g(X)$, i.e.

$$(X^3 + 1)(X^6 + X^5 + X^3 + X^2 + X) + (X^8 + X^3 + X + 1)(X + 1) \;=\; (X + 1)\ ,$$

wie man auch leicht nachrechnet.

Aufgabe 9

Die Formel für die Addition folgt aus

$$\begin{array}{rcl} rf(X) + sg(X) & = & (\sum_{i \geqslant 0}(rf_i + sg_i)X^i)' \\ & = & \sum_{i \geqslant 1} i(rf_i + sg_i)X^{i-1} \\ & = & r \cdot (\sum_{i \geqslant 1} if_i X^{i-1}) + s \cdot (\sum_{i \geqslant 1} ig_i X^{i-1}) \\ & = & rf'(X) + sg'(X)\ . \end{array}$$

Für die Formel für die Multiplikation zeigen wir zunächst, daß sie im Falle $f(X) = X^i$ und $g(X) = X^j$ gilt, wobei $i,\, j \in \mathbf{Z}_{\geqslant 0}$.

Es wird, falls $i \geqslant 1$ und $j \geqslant 1$,

$$\begin{array}{rcl} (X^i X^j)' & = & (X^{i+j})' \\ & = & (i + j)(X^{i+j-1}) \\ & = & i(X^{i-1}) \cdot X^j + X^i \cdot j(X^{j-1}) \\ & = & (X^i)'X^j + X^i(X^j)'\ . \end{array}$$

Falls $i = 0$, so wird $(X^0 X^j)' = (X^j)' = (X^0)'X^j + X^0(X^j)'$. Analog im Fall $j = 0$.

Im allgemeinen Fall wird nun, unter Verwendung der Formel für die Addition

$$\begin{array}{rcl} (f(X)g(X))' & = & ((\sum_{i \geqslant 0} f_i X^i)(\sum_{j \geqslant 0} g_j X^j))' \\ & = & (\sum_{i \geqslant 0} \sum_{j \geqslant 0} f_i g_j X^{i+j})' \\ & = & \sum_{i \geqslant 0} \sum_{j \geqslant 0} f_i g_j (X^{i+j})' \\ & = & \sum_{i \geqslant 0} \sum_{j \geqslant 0} f_i g_j ((X^i)'X^j + X^i(X^j)') \\ & = & \sum_{i \geqslant 0} \sum_{j \geqslant 0} f_i g_j (X^i)'X^j + \sum_{i \geqslant 0} \sum_{j \geqslant 0} f_i g_j X^i(X^j)' \\ & = & (\sum_{i \geqslant 0} f_i (X^i)')(\sum_{j \geqslant 0} g_j X^j) + (\sum_{i \geqslant 0} f_i X^i)(\sum_{j \geqslant 0} g_j (X^j)') \\ & = & (\sum_{i \geqslant 0} f_i X^i)'(\sum_{j \geqslant 0} g_j X^j) + (\sum_{i \geqslant 0} f_i X^i)(\sum_{j \geqslant 0} g_j X^j)' \\ & = & f'(X)g(X) + f(X)g'(X)\ . \end{array}$$

www.uni-koblenz.de/$\sim$kuenzer/galois/galois.html