M. Künzer

Galoistheorie, WS 08/09

Lösung 4

Aufgabe 10

(1) Sei $x \in R \smallsetminus \{0\}$. Wir haben zu zeigen, daß x invertierbar ist. Die Abbildung $R \longrightarrow R$, $r \longmapsto xr$ ist injektiv. Da für $u,\, v \in K$ und $r,\, s \in R$ auch gilt, daß $x(ur+vs) = u(xr) + v(xs)$, ist diese Abbildung K-linear. Nun ist eine K-lineare Abbildung eines endlichdimensionalen Vektorraums in sich, auch als K-linearer Endomorphismus bezeichnet, genau dann injektiv, wenn die Determinante ihrer beschreibenden Matrix bezüglich einer gewählten Basis nicht verschwindet. Dann aber ist diese Matrix invertierbar, was zeigt, daß die fragliche Abbildung auch bijektiv ist.

Da nun insbesondere die Surjektivität der Abbildung $R \longrightarrow R$, $r \longmapsto xr$ nachgewiesen wurde, haben wir unter anderem das Element 1_R im Bild. Somit gibt es ein $r \in R$ so, daß $xr = 1_R$ ist. Mithin ist x invertierbar.

(2) Es ist $n = \dim_{\mathbf{R}} \mathbf{C} = 2$. Zum Beispiel kann man die Basis $(1+\mathrm{i}, 1-\mathrm{i})$ von $\mathbf{C}$ über $\mathbf{R}$ anführen.

Eine solche Basis heißt auch *Normalbasis.* Eventuell werden wir später noch auf Normalbasen für allgemeinere Erweiterungen eingehen.

Aufgabe 11

(1) (a) Falls $b\langle a\rangle \cap b'\langle a\rangle \neq \emptyset$, dann gibt es ein Element $g \in G$ mit $g = ba^k = b'a^{k'}$ für gewisse $k,\, k' \in \mathbf{Z}$. Wir behaupten, daß $b\langle a\rangle = b'\langle a\rangle$. Aus Symmetriegründen genügt es zu zeigen, daß $b\langle a\rangle \subseteq b'\langle a\rangle$. Sei $\ell \in \mathbf{Z}$ gegeben. Wir haben zu zeigen, daß $ba^\ell \in b'\langle a\rangle$. In der Tat ist $b = b'a^{k'-k}$ und also $ba^\ell = ba^{k'-k+\ell} \in b'\langle a\rangle$.

(b) Zunächst einmal halten wir fest, daß Multiplikation mit b von links eine bijektive Abbildung $G \longrightarrow G$, $g \longmapsto bg$ liefert, invertiert von der Multiplikation mit b^{-1} von links. Also ist

$$|b\langle a\rangle| \;=\; |1\langle a\rangle| \;=\; |\{a^k \;:\; k \in \mathbf{Z}\}|\,.$$

Wenn wir für ein $k \in \mathbf{Z}$ mit Division mit Rest $k = \mathrm{o}(a)q + r$ mit $q \in \mathbf{Z}$ und $r \in [0, \mathrm{o}(a)-1]$ schreiben, so erkennen wir, daß

$$a^k \;=\; a^{\mathrm{o}(a)q+r} \;=\; (a^{\mathrm{o}(a)})^q \cdot a^r \;=\; a^r\,.$$

Also ist $\{a^k \;:\; k \in \mathbf{Z}\} = \{a^k \;:\; k \in [0, \mathrm{o}(a)-1]\}$.

Bleibt zu zeigen, daß $a^k \neq a^\ell$ für $0 \leqslant k < \ell \leqslant \mathrm{o}(a)-1$. *Wäre* dem nicht so, dann wäre $a^{\ell-k} = 1$, obwohl $1 \leqslant \ell - k < \mathrm{o}(g)$, im *Widerspruch* zur Minimalität in der Definition von $\mathrm{o}(a)$.

(c) Mit (a) ist G eine disjunkte Vereinigung von Mengen der Form $b\langle a\rangle$ für gewisse $b \in G$. Diese Mengen haben mit (b) aber alle Kardinalität $\mathrm{o}(a)$. Somit ist $|G|$ ein Vielfaches von $\mathrm{o}(a)$.

(2) In $\mathbf{F}_7$ ist

$$\begin{array}{rcr}
3^1 & = & 3 \\
3^2 & = & 2 \\
3^3 & = & -1 \\
3^4 & = & -3 \\
3^5 & = & -2 \\
3^6 & = & 1\,.
\end{array}$$

Wir entnehmen dieser Rechnung, daß

$$\begin{array}{lclcl}
\mathrm{o}(3^1) & = & \mathrm{o}(3) & = & 6 \\
\mathrm{o}(3^2) & = & \mathrm{o}(2) & = & 3 \\
\mathrm{o}(3^3) & = & \mathrm{o}(-1) & = & 2 \\
\mathrm{o}(3^4) & = & \mathrm{o}(-3) & = & 3 \\
\mathrm{o}(3^5) & = & \mathrm{o}(-2) & = & 6 \\
\mathrm{o}(3^6) & = & \mathrm{o}(1) & = & 1\,.
\end{array}$$

Alle diese Elementordnungen sind in der Tat Teiler von $7 - 1 = 6$.

(3) In $\mathbf{F}_{11}$ ist

$$\begin{array}{rcr} 2^1 & = & 2 \\ 2^2 & = & 4 \\ 2^3 & = & -3 \\ 2^4 & = & 5 \\ 2^5 & = & -1 \\ 2^6 & = & -2 \\ 2^7 & = & -4 \\ 2^8 & = & 3 \\ 2^9 & = & -5 \\ 2^{10} & = & 1\,. \end{array}$$

Wir entnehmen dieser Rechnung, daß

$$\begin{array}{lclcr} \mathrm{o}(2^1) & = & \mathrm{o}(2) & = & 10 \\ \mathrm{o}(2^2) & = & \mathrm{o}(4) & = & 5 \\ \mathrm{o}(2^3) & = & \mathrm{o}(-3) & = & 10 \\ \mathrm{o}(2^4) & = & \mathrm{o}(5) & = & 5 \\ \mathrm{o}(2^5) & = & \mathrm{o}(-1) & = & 2 \\ \mathrm{o}(2^6) & = & \mathrm{o}(-2) & = & 5 \\ \mathrm{o}(2^7) & = & \mathrm{o}(-4) & = & 10 \\ \mathrm{o}(2^8) & = & \mathrm{o}(3) & = & 5 \\ \mathrm{o}(2^9) & = & \mathrm{o}(-5) & = & 10 \\ \mathrm{o}(2^{10}) & = & \mathrm{o}(1) & = & 1\,. \end{array}$$

Alle diese Elementordnungen sind in der Tat Teiler von $11 - 1 = 10$.

Aufgabe 12

(1) Ist $a = 0$, so ist $0^p = 0$.

Ist $a \neq 0$, so ist mit Aufgabe 11.(1.c) ist $\mathrm{o}(a)$ ein Teiler von $|\mathbf{F}_p^\times| = p - 1$, sagen wir $p - 1 = \mathrm{o}(a) \cdot m$ mit $m \in \mathbf{Z}_{\geqslant 1}$. Dann wird

$$a^{p-1} \;=\; a^{\mathrm{o}(a)\cdot m} \;=\; (a^{\mathrm{o}(a)})^m \;=\; 1\,,$$

und also $a^p = p$.

(2) Es hat mit (1) das Polynom $X^p - X$ die Nullstellen $i \in \mathbf{F}_p$. Also zeigt sukzessives Abdividieren von Nullstellen, daß die linke Seite ein Vielfaches der rechten Seite ist. Da linke und rechte Seite normierte Polynome vom gleichen Grad p sind, ist die linke Seite gleich der rechten Seite.

Zum Beispiel wird $\prod_{i\in[0,3-1]}(X-i) = X^3 - 3X^2 + 2X$ in $\mathbf{Z}[X]$, und also in der Tat $\prod_{i\in\mathbf{F}_3}(X-i) = X^3 - X$ in $\mathbf{F}_3[X]$.

(3) Für $p = 2$ ist $(2-1)! = 1 \equiv_2 -1$.

Sei nun $p \geqslant 3$. Der Koeffizient von X auf der linken Seite von (2) ist gleich -1. Der Koeffizient von X auf der rechten Seite dagegen ist gleich $\prod_{i\in\mathbf{F}_p^\times} i$. Somit ist $-1 = \prod_{i\in\mathbf{F}_p^\times} i$ in $\mathbf{F}_p$. In anderen Worten, es ist $-1 \equiv_p (p-1)!$ in $\mathbf{Z}$.

Hingegen ist $(4-1)! = 6 \not\equiv_4 -1$. Also ist $(n-1)! \equiv_n -1$ für alle $n \in \mathbf{Z}_{\geqslant 1}$ nicht für alle $n \in \mathbf{Z}_{\geqslant 1}$ richtig.

Man kann alternativ auch die Elemente von $\mathbf{F}_p^\times$ außer 1 und -1 zu sich invertierenden Paaren sortieren – beachte, daß das Polynom $X^2 = 1$ nur diese beiden Nullstellen aufweist, und daher in diesen Paaren jeweils zwei verschiedene Elemente stehen. Das Produkt über alle Elemente von $\mathbf{F}_p^\times$ ist also gleich

$$1 \cdot (-1) \cdot (\text{Produkt aller dieser Paareinträge}) \;=\; 1 \cdot (-1) \cdot 1 \;=\; -1\,.$$

(4) Der Koeffizient von X^2 auf der linken Seite von (2) ist gleich 0, da $p \geqslant 3$. Der Koeffizient von X^2 auf der rechten Seite dagegen ist gleich

$$-\sum_{j\in\mathbf{F}_p^\times}\prod_{i\in\mathbf{F}_p^\times\smallsetminus\{j\}} i\ .$$

Es folgt $0 \equiv_p \sum_{j\in[1,p-1]}\frac{(p-1)!}{j} =: t(p)$ in $\mathbf{Z}$. Nun ist $s(p) = \frac{t(p)}{(p-1)!}$. Da $t(p)$ durch p teilbar ist, nicht aber $(p-1)!$, liefert auch vollständiges Kürzen einen durch p teilbaren Zähler von $s(p)$ in gekürzter Form.

Der Zähler von $s(p)$ ist für $p \geqslant 5$ sogar durch p^2 teilbar (Hinweis von G. Nebe; Theorem von Wolstenholme). Betrachte hierzu

$$\begin{array}{rcl} 2\cdot s(p) & = & (\frac{p}{1\cdot(p-1)}+\frac{1}{p-1})+(\frac{1}{2}+\frac{1}{p-2})+\cdots+(\frac{1}{p-1}+\frac{1}{1}) \\ & = & \frac{p}{1\cdot(p-1)}+\frac{p}{2\cdot(p-2)}+\cdots+\frac{p}{(p-1)\cdot 1}\ . \end{array}$$

Wir haben also zu zeigen, daß $\frac{1}{1\cdot(p-1)}+\frac{1}{2\cdot(p-2)}+\cdots+\frac{1}{(p-1)\cdot 1}$ in gekürzter Form einen durch p teilbaren Nenner hat. Es genügt hierzu zu zeigen, daß die ganze Zahl

$$\frac{(p-1)!}{1}\cdot\frac{(p-1)!}{(p-1)}+\frac{(p-1)!}{2}\cdot\frac{(p-1)!}{(p-2)}+\cdots+\frac{(p-1)!}{(p-1)}\cdot\frac{(p-1)!}{1}$$

durch p teilbar ist. Nun ist $\frac{(p-1)!}{p-a}+\frac{(p-1)!}{a} = (p-1)!\frac{p}{(p-a)a}$ eine durch p teilbare ganze Zahl für $a\in[1,p-1]$, und mithin $\frac{(p-1)!}{p-a}\equiv_p -\frac{(p-1)!}{a}$. Also genügt es nach Ersetzung der jeweiligen zweiten Faktoren zu zeigen, daß

$$\frac{(p-1)!^2}{1^2}+\frac{(p-1)!^2}{2^2}+\cdots+\frac{(p-1)!^2}{(p-1)^2}$$

durch p teilbar ist.

Koeffizientenvergleich bei X^3 in (2) liefert, da $p \geqslant 5$, daß $0 \equiv_p \sum_{0\leqslant i<j\leqslant p-1}\frac{(p-1)!}{ij}$. Also teilt p nach Multiplikation mit $2(p-1)!$ auch

$$\sum_{i,\,j\,\in\,[0,p-1],\,i\neq j}\frac{(p-1)!^2}{ij}$$

Aus (3) wissen wir, daß p (und sogar p^2) ein Teiler von

$$\sum_{i,\,j\,\in\,[0,p-1]}\frac{(p-1)!^2}{ij} \;=\; (\sum_{i\in[0,p-1]}\frac{(p-1)!}{i})^2$$

ist. Somit teilt p auch die Differenz dieser beiden Ausdrücke, und das ist gerade

$$\sum_{i\in[0,p-1]}\frac{(p-1)!^2}{i^2} \;=\; \frac{(p-1)!^2}{1^2}+\frac{(p-1)!^2}{2^2}+\cdots+\frac{(p-1)!^2}{(p-1)^2}\ .$$