Blatt 3, Aufgabe (2)

Sei K ein Körper.

(a) Sei $G = \{\sigma_1, \dots, \sigma_n\}$ eine Menge paarweise verschiedener Automorphismen von K. $K^G := \{a \in K : \sigma_j(a) = a \text{ für } j = 1, \dots, n\}$.

Behauptung: $[K : K^G] \geq n$

Achtung: G ist eine Menge, keine Gruppe. Die kleinste Gruppe, die G enthält, kann schon unendlich sein. Proposition 1.4 ist also nicht anwendbar.

Hinweis in der Aufgabenstellung: lineare Algebra!

Beweis der Behauptung:

Angenommen $[K : K^G] = r < n$. Sei $b_1, \dots, b_r$ eine K^G-Basis von K.

Auf die b_i wenden wir die σ_j an und schreiben ein homogenes lineares Gleichungssystem auf mit Variablen $x_1, \dots, x_n$ und Koeffizienten $\sigma_j(b_i) \in K$:

↑ nachprüfen: K^G ist ein Körper

$$\left.\begin{aligned} \sigma_1(b_1)x_1 + \dots + \sigma_n(b_1)x_n &= 0 \\ \sigma_1(b_2)x_1 + \dots + \sigma_n(b_2)x_n &= 0 \\ \vdots \qquad\qquad & \qquad \vdots \\ \sigma_1(b_r)x_1 + \dots + \sigma_n(b_r)x_n &= 0 \end{aligned}\right\} \begin{array}{l} \text{in Variablen} \\ r < n \text{ Gleichungen} \end{array} \quad (*)$$

Es gibt nichttriviale Lösungen, wir wählen eine und nennen sie $(x_1, \dots, x_n)$.

Jedes Element $c \in K$ ist eine Linearkombination

$$c = \sum_{i=1}^{r} \lambda_i b_i \text{ mit } \lambda_1, \dots, \lambda_r \in K^G, \text{ d.h. } \sigma_i(\lambda_j) = \lambda_j \ \forall i, j$$

$\Rightarrow$ Wir können die Gleichungen in $(*)$ mit $\lambda_1, \dots, \lambda_r$ multiplizieren und diese als Koeffizienten als $\lambda_i = \sigma_1(\lambda_i) = \sigma_j(\lambda_i)$ schreiben und erhalten als i-te Gleichung $\sigma_1(\lambda_i b_i)x_1 + \dots + \sigma_n(\lambda_i b_i)x_n = 0$.

Aufaddieren aller Gleichungen ergibt (mit $c = \sum \lambda_i b_i$)

$$\sigma_1(c)x_1 + \dots + \sigma_n(c)x_n = 0 \quad (\text{für jedes } c)$$

Anders gesagt: Die Funktion $x_1\sigma_1 + \dots + x_n\sigma_n : K \longrightarrow K$ ist die Nullfunktion.

Wir suchen nach einem Widerspruch, und jetzt ist unsere Chance gekommen:
Ein Automorphismus $\sigma_i \in Aut(K)$ bildet K in $K\setminus\{0\}$, 0 in 0, also $K^* = \{a \in K : a \neq 0, \text{bzw. } a \text{ invertierbar}\}$ in K^*, und $K^* \subset K$.
K^* ist eine (multiplikative) Gruppe.
$\Rightarrow \sigma_1, \dots, \sigma_n$ (eingeschränkt auf K^*) sind Charaktere der multiplikativen Gruppe K^* mit Werten in K. (Gruppenhomomorphismen)
In Proposition 2.4 haben wir gezeigt: Paarweise verschiedene Charaktere $\sigma_1, \dots, \sigma_n$ sind linear unabhängig. Damit ist der Widerspruch erreicht und die Behauptung ist bewiesen.

(b) Jetzt ist $G = \{\sigma_1, \dots, \sigma_n\}$ eine Gruppe.
Behauptung: $[K : K^G] = |G|$.
Wir könnten 1.4 anwenden (eine ziemlich schwierig zu beweisende Aussage), aber der Hinweis sagt wieder, daß wir lineare Algebra benutzen sollen. Damit bekommen wir einen unabhängigen Beweis dieser Aussage. (Das war in der Aufgabe nicht verlangt.)
Beweis der Behauptung:
Wegen (a) reichts $[K : K^G] \leq |G| = n$ zu zeigen.
Angenommen $[K : K^G] > n$. Dann gibt es $n+1$ Vektoren $w_1, \dots, w_{n+1}$ in K, die über K^G linear unabhängig sind.
Wir recyclen die Idee aus dem Beweis von (a), die ja offenbar gut war, und schreiben wieder ein homogenes lineares Gleichungssystem auf:

$$\left.\begin{array}{ccc} \sigma_1(w_1)x_1 + \dots + \sigma_1(w_{n+1})x_{n+1} = 0 \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ \sigma_n(w_1)x_1 + \dots + \sigma_n(w_{n+1})x_{n+1} = 0 \end{array}\right\} \begin{array}{l} n+1 \text{ Variablen} \\ n \text{ Gleichungen} \end{array} \quad (**)$$

Wieder sind es mehr Variablen als Gleichungen. Deshalb gibt es wieder eine nichttriviale Lösung, die wir $(x_1, \dots, x_{n+1})$ nennen. Natürlich kann es viele solche Lösungen geben. Wir wählen eine aus, die möglichst wenige Einträge $\neq 0$ hat, aber natürlich mindestens einen.

Da wir die Reihenfolge der Vektoren $w_1, \dots, w_{n+1}$ frei wählen dürfen, können wir so eine Lösung als $(x_1, \dots, x_r, 0, \dots, 0)$ schreiben mit minimalem $r \geq 0$. r muß sogar größer als 1 sein: $r=1$ würde bedeuten, daß $(**)$ die Gleichung $\sigma_1(w_1) x_1 = 0$ enthält, aber $w_1 \neq 0$, $\sigma_1(w_1) \neq 0 \Rightarrow x_1 = 0$ $\lightning$.
$\rightsquigarrow (x_1, \dots, x_r, 0, \dots, 0)$. Die Lösungsmenge ist ein Vektorraum $\Rightarrow$ wir können $x_r = 1$ annehmen.
mindestens 2 Einträge. Können noch normalisieren und

Die $x_1, \dots, x_r$ liegen nach Definition in K. Sie können nicht alle in K^G liegen, denn: ein σ ist die Identität (G Gruppe) und dazu gehört in $(**)$ die Gleichung $\underbrace{w_1 x_1 + \dots}_{\text{id}(w_1)} + \underbrace{w_r x_r}_{\text{id}(w_r)} + 0 + \dots + 0 = 0$, aber $w_1, \dots$ sind über K^G linear unabhängig.

Also ist ein $x_i \notin K^G$, der wählen wir als x_1 (nochmaliges Umsortieren).
K^G = Fixkörper $\Rightarrow \exists \sigma_k : \sigma_k(x_1) \neq x_1$.
($x_1 = 1$ dagegen liegt natürlich in K^G.)
Jetzt folgen Standard-Umformungen bei linearen Gleichungssystemen: Wir multiplizieren Gleichungen mit Skalaren, subtrahieren sie voneinander und finden eine nichttriviale Lösung mit weniger als r Einträgen $\neq 0$ – das ist der gesuchte Widerspruch.
Im Detail: Die j-te Zeile in $(**)$ ist

$$\sigma_j(w_1) x_1 + \dots + \sigma_j(w_{r-1}) x_{r-1} + \sigma_j(w_r) \cdot 1 = 0$$

$\xrightarrow{\sigma_k \text{ anwenden}}$ (umsortiertes lineares System)

$$\sigma_k\sigma_j(w_1)\sigma_k(x_1) + \dots + \sigma_k\sigma_j(w_{r-1})\sigma_k(x_{r-1}) + \sigma_k\sigma_j(w_r) = 0$$

G Gruppe $\Rightarrow G = \{\sigma_k\sigma_1, \sigma_k\sigma_2, \dots, \sigma_k\sigma_n\}$, z.B. $\sigma_k\sigma_j = \sigma_i$, dann steht in der i-ten Zeile des umsortierten Systems $\sigma_i(w_1)\sigma_k(x_1) + \dots + \sigma_i(w_{r-1})\sigma_k(x_{r-1}) + \sigma_i(w_r) = 0$
und in $(**)$ $\sigma_i(w_1) x_1 + \dots + \sigma_i(w_{r-1}) x_{r-1} + \sigma_i(w_r) = 0$
Subtrahieren $\Rightarrow$ $\sigma_i(w_1)\underbrace{[x_1 - \sigma_k(x_1)]}_{\neq 0} + \dots + \sigma_i(w_{r-1})[x_{r-1} - \sigma_k(x_{r-1})] + 0 - 0 = 0$

$(x_1, \dots, x_r, 0, \dots, 0)$ und $(\sigma_k(x_1), \dots, \sigma_k(x_r), 0, \dots, 0)$ sind Lösungen, die Differenz $(x_1 - \sigma_k(x_1), \dots, x_{r-1} - \sigma_k(x_{r-1}), 0, \dots, 0)$ ist auch eine Lösung, auch nicht-trivial, aber mit weniger Einträgen $\neq 0$. $\lightning$

Jetzt dürfen wir natürlich nicht aufgeben, sondern müssen auch noch Teil (c) ohne Einsatz von 1.4 lösen:

(c) Seien G und H endliche Untergruppen von $\mathrm{Aut}(K)$ mit $K^G = K^H$.

Behauptung: $G = H$.

Beweis der Behauptung:

Sei $\sigma \in \mathrm{Aut}(K)$. Wenn $\sigma \in G$ und $a \in K^G$, dann ist $a = \sigma(a)$, nach Definition.

Wir zeigen die Umkehrung: $a = \sigma(a) \ \forall a \in K^G \Rightarrow \sigma \in G$.

Angenommen $\sigma \notin G$. Sei $|G| = n$ $\overset{(4)}{\Rightarrow}$ $[K : K^G] = n = |G|$.

Wir vergrößern G zu $X = G \cup \{\sigma\}$, also $|X| = n+1$. Nach Wahl von σ ist $K^G \subset K^X$, aber $X > G \Rightarrow K^X \subset K^G$ (nach Definition der Fixkörper).

Nun sehen wir, daß es sich gelohnt hat, in (c) endliche Mengen zu betrachten, nicht nur Gruppen:

$n = [K : K^G] = [K : K^X] \overset{(a)}{\geq} |X| = n+1 \Rightarrow n \geq n+1$ ↯.

Daraus folgt $\sigma \in G$.

Wegen $K^H = K^G$ folgt $\sigma \in G \ \forall \sigma \in H$, damit $H \subset G$ und natürlich analog $G \subset H$, daher $H = G$.