D-MATH | Algebra II | FS 2023
Prof. Richard Pink

Musterlösung Serie 20

Sylowsätze und kleine Gruppen, Körperhomomorphismen, Zerfällungskörper

1. (a) Zeige, dass jede endliche Gruppe G mit einer nicht-trivialen zyklischen 2-Sylowuntergruppe eine normale Untergruppe vom Index 2 hat.

   Hinweis: Betrachte G als Untergruppe der symmetrischen Gruppe $S(G)$ nach dem Satz von Cayley und achte auf das Vorzeichen.

   (b) Folgere daraus, dass eine nicht-abelsche endliche Gruppe der Ordnung $\equiv 2 \mod 4$ nicht einfach sein kann.

   Lösung:

   (a) Wie im Beweis des Satzes von Cayley betrachten wir die Operation von G auf G durch Linkstranslation. Diese Operation ist frei und treu und entspricht einem injektiven Homomorphismus

$$\begin{aligned} \ell\colon G &\longrightarrow S(G) \\ x &\longmapsto \ell_x\colon g \mapsto xg. \end{aligned}$$

   Nach Voraussetzung hat G eine nicht-triviale zyklische 2-Sylowgruppe $P = \langle x\rangle$. Also ist $|P| = 2^k$ für ein $k > 0$ und $|G| = 2^k m$ mit m ungerade. Jede Bahn von P hat dann die Form Pg für ein $g \in G$ und folglich die Kardinalität $|Pg| = |P| = 2^k$. Die Permutation $\ell_x \in S(G)$ ist daher ein Produkt von m disjunkten 2^k-Zykeln. Als Zykeln gerader Länge sind diese 2^k-Zykel ungerade, und da auch m ungerade ist, folgt

$$\operatorname{sgn}(\ell_x) = (-1)^m = -1.$$

   Darum ist der zusammengesetzte Homomorphismus $\operatorname{sgn} \circ \ell : G \to \{\pm 1\}$ surjektiv und sein Kern nach dem Homomorphiesatz ein Normalteiler vom Index 2.

   (b) Sei G eine nicht-abelsche Gruppe der Ordnung $n \equiv 2 \bmod 4$. Jede 2-Sylowgruppe einer solchen Gruppe hat die Ordnung 2 und ist daher zyklisch. Somit hat G nach (a) eine normale Untergruppe vom Index 2. Diese ist nicht trivial, da G als nicht-abelsche Gruppe nicht die Ordnung 2 haben kann. Daher ist G nicht einfach.

2. Zeige, dass jede Gruppe der folgenden Ordnung auflösbar ist:

   (a) $|G| = 4 \cdot 3 \cdot 7$.

   (b) $|G| = 16 \cdot 5$

   (c) $|G| = 8 \cdot 5 \cdot 7$

**(d) $|G| = 16 \cdot 5 \cdot 7$

**(e) $|G| = 4 \cdot 3 \cdot 11 \cdot 13$

Lösung:

(a) Für $|G| = 4 \cdot 3 \cdot 7$ ist die Anzahl der 7-Sylowgruppen ein Teiler von $4 \cdot 3$ und kongruent zu 1 modulo (7). Die einzige Möglichkeit dafür ist 1. Somit besitzt G eine normale 7-Sylowgruppe P. Die Faktorgruppe G/P hat dann die Ordnung $2^2 \cdot 3$ und ist daher auflösbar nach einem Satz der Vorlesung. Somit ist auch G auflösbar.

(b) Für $|G| = 16 \cdot 5$ ist die Anzahl a der 5-Sylowgruppen ein Teiler von 16 und kongruent zu 1 modulo (5). Die einzigen Möglichkeiten dafür sind $a \in \{1, 16\}$.

Im Fall $a = 1$ besitzt G eine normale 5-Sylowgruppe P, und die Faktorgruppe G/P hat die Ordnung 16 und ist daher als p-Gruppe auflösbar. Somit ist auch G auflösbar.

Im Fall $a = 16$ besitzt G genau 16 verschiedene 5-Sylowgruppen, und jede davon enthält genau $5 - 1 = 4$ verschiedene Elemente der Ordnung 5. Umgekehrt liegt jedes Element der Ordnung 5 in genau einer 5-Sylowgruppe. Somit besitzt G genau $16 \cdot 4$ Elemente der Ordnung 5. Damit verbleiben genau 16 Elemente der Ordnung $\neq 5$. Aber jede 2-Sylowgruppe Q von G besteht schon aus 16 Elementen. Daher besteht diese genau aus allen Elemente der Ordnung $\neq 5$ und ist somit normal in G. Nun ist Q als p-Gruppe auflösbar, und da G/Q als Gruppe der Primzahlordnung 5 abelsch ist, ist G auflösbar.

(c) Für $|G| = 8 \cdot 5 \cdot 7$ ist die Anzahl a der 7-Sylowgruppen ein Teiler von $8 \cdot 5$ und kongruent zu 1 modulo (7). Die einzigen Möglichkeiten dafür sind $a \in \{1, 8\}$.

Im Fall $a = 1$ besitzt G eine normale 7-Sylowgruppe P und die Faktorgruppe G/P hat die Ordnung $8 \cdot 5 = 40$. In der Vorlesung wurde schon gezeigt, dass diese auflösbar ist. Da P abelsch ist, ist damit auch G auflösbar.

Im Fall $a = 8$ betrachte eine 7-Sylowgruppe $P < G$ und ihren Normalisator $N := \mathrm{Norm}_G(P)$. Dann ist $[G : N] = 8$ und folglich $|N| = |G|/8 = 5 \cdot 7$. Die Anzahl der 5-Sylowgruppen von N (sic!) ist dann ein Teiler von 7 und kongruent zu 1 modulo (5). Die einzige Möglichkeit dafür ist 1. Somit besitzt N eine normale 5-Sylowgruppe Q. Mit $M := \mathrm{Norm}_G(Q)$ gilt dann $N < M$. Daher ist $|\operatorname{Syl}_5(G)| = [G : M]$ ein Teiler von $[G : N] = 8$. Da die Anzahl der 5-Sylowgruppen von G aber kongruent zu 1 modulo (5) ist, bleibt dafür nur die Möglichkeit 1. Somit ist $Q \lhd G$. Nun ist Q abelsch und die Faktorgruppe G/Q als Gruppe der Ordnung $8 \cdot 7 = 56$ auflösbar nach der Vorlesung. Also ist auch G auflösbar.

**(d) $|G| = 16 \cdot 5 \cdot 7$ weggelassen

**(e) $|G| = 4 \cdot 3 \cdot 11 \cdot 13$ weggelassen

*3. Zeige, dass jede Gruppe der Ordnung $2^2 \cdot 3 \cdot 7 \cdot 13 \cdot 17$ eine normale Untergruppe der Ordnung 17 hat.

Hinweis: Finde eine 13-Sylowgruppe P und eine 17-Sylowgruppe Q von G mit $Q < \mathrm{Norm}_G(P)$ und untersuche dann $\mathrm{Norm}_G(Q)$.

Lösung: Sei G eine Gruppe der Ordnung $2^2 \cdot 3 \cdot 7 \cdot 13 \cdot 17$. Nach den Sylowsätzen ist die Anzahl der 13-Sylowgruppen von G ein Teiler von $2^2 \cdot 3 \cdot 7 \cdot 17$ und kongruent zu 1 modulo 13. Nachrechnen ergibt dafür nur die Möglichkeiten 1 und $2 \cdot 7$. Diese Zahl ist jedenfalls kein Vielfaches von 17.

Sei P eine beliebige 13-Sylowgruppe von G. Ihr Normalisator $\mathrm{Norm}_G(P)$ ist der Stabilisator von P bezüglich der Operation von G durch Konjugation auf der Menge der 13-Sylowgruppen von G. Da diese Operation nach den Sylowsätzen transitiv ist, ist der Index $[G : \mathrm{Norm}_G(P)]$ gleich der Anzahl von 13-Sylowgruppen. Nach obiger Rechnung ist also $[G : \mathrm{Norm}_G(P)]$ nicht durch 17 teilbar. Da aber 17 ein Teiler von der Ordnung von G ist, muss darum $|\,\mathrm{Norm}_G(P)|$ durch 17 teilbar sein. Somit enthält $\mathrm{Norm}_G(P)$ ein Element der Ordnung 17 und daher eine Untergruppe Q der Ordnung 17.

Die Operation von Q auf $P \cong \mathbb{Z}/13\mathbb{Z}$ entspricht dann einem Homomorphismus $Q \to (\mathbb{Z}/13\mathbb{Z})^\times$. Da $|Q| = 17$ und $|(\mathbb{Z}/13\mathbb{Z})^\times| = 12$ zueinander teilerfremd sind, muss dieser Homomorphismus trivial sein. Somit kommutieren P und Q miteinander. Daraus folgt insbesondere $P < \mathrm{Norm}_G(Q)$. Daher ist $|P| = 13$ ein Teiler von $|\,\mathrm{Norm}_G(Q)|$ und somit kein Teiler des Indexes $[G : \mathrm{Norm}_G(Q)]$.

Als Untergruppe der Ordnung 17 ist Q nun aber eine 17-Sylowgruppe von G. Nach demselben Argument wie oben ist die Anzahl der 17-Sylowgruppen daher gleich dem Index $[G : \mathrm{Norm}_G(Q)]$, also kein Vielfaches von 13. Nach den Sylowsätzen ist diese Anzahl aber ein Teiler von $2^2 \cdot 3 \cdot 7 \cdot 13$ und kongruent zu 1 modulo 17. Nachrechnen ergibt dafür nur die Möglichkeiten 1, $4 \cdot 13$ und $3 \cdot 7 \cdot 13$. Da diese Anzahl auch kein Vielfaches von 13 sein darf, muss sie daher gleich 1 sein. Dies bedeutet, dass Q als einzige 17-Sylowgruppe normal in G ist, was zu zeigen war.

**4. (a) Zeige, dass es keine nicht-abelsche einfache Gruppe mit $60 < |G| < 168$ gibt.

(b) Zeige, dass jede einfache Gruppe der Ordnung 168 isomorph zu $\mathrm{PSL}_2(\mathbb{F}_7)$ ist.

Lösung: weggelassen

5. Seien $a, b \in \mathbb{C}$ zwei verschiedene dritte Wurzeln von 2 und sei $i \in \mathbb{C}$ die imaginäre Einheit mit $i^2 = -1$. Bestimme alle Körperhomomorphismen

(a) $\mathbb{Q}(a, i) \to \mathbb{C}$.

(b) $\mathbb{Q}(a, b) \to \mathbb{C}$.

Lösung: Zur Vorbereitung bestimmen wir alle Homomorphismen $\mathbb{Q}(a) \to \mathbb{C}$. Nach dem Eisensteinkriterium für $p = 2$ ist das Polynom $X^3 - 2$ irreduzibel über $\mathbb{Q}$.

Da es normiert ist und die Nullstelle a hat, ist es das Minimalpolynom von a über $\mathbb{Q}$. Ausserdem ist $\mathbb{Q}(a)$ ein Stammkörper von $X^3 - 2$ über $\mathbb{Q}$. Da dieser bis auf Isomorphie von der Wahl der Nullstelle unabhängig ist, und es eine reelle Nullstelle gibt, besitzt $\mathbb{Q}(a)$ eine Einbettung nach $\mathbb{R}$, egal ob a selbst schon reell ist oder nicht.

Nun ist jeder Homomorphismus $\mathbb{Q}(a) \to \mathbb{C}$ ein Homomorphismus über dem Primkörper $\mathbb{Q}$. Nach Abschnitt 6.2 der Vorlesung sind diese Homomorphismen daher in Bijektion mit der Menge $\{z \in \mathbb{C} \mid z^3 = 2\}$ aller komplexen dritten Wurzeln aus 2.

(a) Da $\mathbb{Q}(a)$ nach $\mathbb{R}$ eingebettet werden kann, das quadratische Polynom $Y^2 + 1$ aber keine Nullstelle in $\mathbb{R}$ besitzt, hat das Polynom auch keine Nullstelle in $\mathbb{Q}(a)$ und ist daher irreduzibel über $\mathbb{Q}(a)$. Somit ist $Y^2 + 1$ das Minimalpolynom von i über $\mathbb{Q}(a)$.

Wähle nun einen Körperhomomorphismus $\mathbb{Q}(a) \to \mathbb{C}$ wie oben und betrachte $\mathbb{C}$ via diesen als Körpererweiterung von $\mathbb{Q}(a)$. Nach Abschnitt 6.2 der Vorlesung stehen die Körperhomomorphismen $\mathbb{Q}(a,i) \to \mathbb{C}$ über $\mathbb{Q}(a)$ dann in Bijektion mit der Menge $\{w \in \mathbb{C} \mid w^2 = -1\}$. Insgesamt stehen die Körperhomomorphismen $\mathbb{Q}(a,i) \to \mathbb{C}$ daher in Bijektion mit der Produktmenge

$$\big\{(z,w) \in \mathbb{C}^2 \bigm| z^3 = 2,\ w^2 = -1\big\}.$$

Jedes solche Paar (z,w) entspricht dabei einem eindeutigen Homomorphismus $\varphi\colon \mathbb{Q}(a,i) \to \mathbb{C}$ mit $\varphi(a) = z$ und $\varphi(i) = w$.

(b) Sei c die dritte Nullstelle von $X^3 - 2$. Da das Polynom $X^3 - 2$ die Nullstelle $a \in \mathbb{Q}(a)$ hat, besitzt es eine Faktorisierung $X^3 - 2 = (X - a) \cdot g(X)$ für ein normiertes Polynom $g(X) \in \mathbb{Q}(a)[X]$ vom Grad 2 mit den komplexen Nullstellen b und c. Da $\mathbb{Q}(a)$ nach $\mathbb{R}$ eingebettet werden kann, aber $b/a = \exp(\pm\frac{2\pi i}{3})$ nicht, liegt b nicht schon in $\mathbb{Q}(a)$. Somit ist g irreduzibel über $\mathbb{Q}(a)$ und daher das Minimalpolynom von b über $\mathbb{Q}(a)$.

Wähle nun einen Körperhomomorphismus $\psi\colon \mathbb{Q}(a) \to \mathbb{C}$ wie oben und betrachte $\mathbb{C}$ via diesen als Körpererweiterung von $\mathbb{Q}(a)$. Das Bild von g unter dem von ψ induzierten Ringhomomorphismus $\mathbb{Q}(a)[X] \to \mathbb{C}[X]$ hat dann die Form $\psi(g) = (X^3 - 2)/(X - \varphi(a))$. Nach Abschnitt 6.2 der Vorlesung stehen die Homomorphismen $\mathbb{Q}(a,b) \to \mathbb{C}$ über $\mathbb{Q}(a)$ via ψ in Bijektion mit der Menge $\{w \in \mathbb{C} \mid \psi(g)(w) = 0\}$. Dies ist genau die Menge der von $\psi(a)$ verschiedenen dritten Wurzeln aus 2. Insgesamt stehen die Körperhomomorphismen $\mathbb{Q}(a,b) \to \mathbb{C}$ daher in Bijektion mit der Menge aller Paare

$$\big\{(z,w) \in \mathbb{C}^2 \bigm| z^3 = w^3 = 2,\ z \neq w\big\}.$$

Jedes solche Paar (z,w) entspricht dabei einem eindeutigen Homomorphismus $\varphi\colon \mathbb{Q}(a,b) \to \mathbb{C}$ mit $\varphi(a) = z$ und $\varphi(b) = w$. Dieser Homomorphismus muss dann die übrige dritte Wurzel aus 2 auf die von z und w verschiedene dritte Wurzel aus

2 abbilden. Die Homomorphismen entsprechen daher genau den Permutationen der Menge $\{z \in \mathbb{C} \mid z^3 = 2\}$.

6. Zeige, dass $\mathrm{id}_{\mathbb{R}}$ der einzige Körperendomorphismus von $\mathbb{R}$ ist.

   Lösung: Sei φ ein Körperendomorphismus von $\mathbb{R}$. Da $\mathbb{Q}$ der Primkörper von $\mathbb{R}$ ist, gilt $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.

   Wir zeigen nun, dass φ streng monoton ist: Seien $x, y \in \mathbb{R}$ mit $x > y$. Wegen $x - y > 0$ existiert dann ein $z \in \mathbb{R}$ mit $z^2 = x - y$. Dann ist $\varphi(z)^2 = \varphi(x) - \varphi(y)$, und da φ injektiv ist, gilt $\varphi(z) \neq 0$. Daraus folgt $\varphi(x) - \varphi(y) > 0$, also $\varphi(x) > \varphi(y)$, und somit ist φ streng monoton.

   Für jedes $x \in \mathbb{R}$ und jedes $\varepsilon > 0$ existieren $x_1, x_2 \in \mathbb{Q}$ mit

   $$x - \varepsilon < x_1 < x < x_2 < x + \varepsilon.$$

   Wegen der Monotonie von φ und mit $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ folgt

   $$x - \varepsilon < x_1 = \varphi(x_1) < \varphi(x) < \varphi(x_2) = x_2 < x + \varepsilon.$$

   Daraus folgt $|x - \varphi(x)| < \varepsilon$. Da $\varepsilon > 0$ beliebig war, muss also $\varphi(x) = x$ sein.

7. (a) Beweise, dass $(X^2 - 2X - 2)(X^2 + 1)$ und $X^5 - 3X^3 + X^2 - 3$ dieselben Zerfällungskörper K über $\mathbb{Q}$ haben, und finde $[K/\mathbb{Q}]$.

   (b) Bestimme den Grad eines Zerfällungskörpers des Polynoms $X^3 + X^2 + 1$ über $\mathbb{Q}$ und über $\mathbb{F}_2$.

   Lösung: (a) Das erste Polynom zerlegt sich über $\mathbb{C}$ in die Linearfaktoren

   $$(X^2 - 2X - 2) \cdot (X^2 + 1) \;=\; (X - 1 + \sqrt{3}) \cdot (X - 1 - \sqrt{3}) \cdot (X - i) \cdot (X + i).$$

   Es besitzt also den Zerfällungskörper $K := \mathbb{Q}(\sqrt{3}, i) \subset \mathbb{C}$. Das zweite Polynom zerlegt sich zu

   $$\begin{aligned} &X^5 - 3X^3 + X^2 - 3 \\ &\quad= (X^2 - 3) \cdot (X^3 + 1) \\ &\quad= (X - \sqrt{3}) \cdot (X + \sqrt{3}) \cdot (X + 1) \cdot (X + \tfrac{1}{2}(-1 + i\sqrt{3})) \cdot (X + \tfrac{1}{2}(-1 - i\sqrt{3})). \end{aligned}$$

   Es besitzt also den Zerfällungskörper $L := \mathbb{Q}(\sqrt{3}, \frac{1}{2}(-1 + i\sqrt{3})) \subset \mathbb{C}$. Die Erzeugenden von L sind offenbar in K enthalten, also gilt $L \subset K$. Umgekehrt sind wegen

   $$i \;=\; \Big(2\Big(\frac{1}{2}(-1 + i\sqrt{3})\Big) + 1\Big) \cdot \frac{\sqrt{3}}{3}$$

   die Erzeugenden von K in L enthalten, also haben wir $K = L$.

   Das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}$ ist $X^2 - 3$, also gilt $[\mathbb{Q}(\sqrt{3})/\mathbb{Q}] = 2$. Da i nicht in der reellen Erweiterung $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ liegt, ist $X^2 + 1$ das Minimalpolynom von i über $\mathbb{Q}(\sqrt{3})$. Folglich gilt $[\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}(\sqrt{3})] = 2$. Wegen der Multiplikativität des Körpergrades haben wir also

$$[K/\mathbb{Q}] = [K/\mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3})/\mathbb{Q}] = 4.$$

(b) *Über* $\mathbb{Q}$*:* Das Polynom $f(X) := X^3 + X^2 + 1$ ist ganzzahlig und normiert. Jede rationale Nullstelle ist somit ganz und ein Teiler des konstanten Koeffizienten. Aber ± 1 sind keine Nullstellen; also hat f keine Nullstelle in $\mathbb{Q}$. Wegen $\deg(f) = 3$ ist es deshalb schon irreduzibel über $\mathbb{Q}$.

Da $\deg(f) = 3$ ungerade ist, besitzt f mindestens eine reelle Nullstelle a. Um zu untersuchen, ob die anderen beiden Nullstellen ebenfalls in $\mathbb{R}$ liegen, wenden wir Methoden der Analysis an. Die erste Ableitung von f ist $f'(X) = 3X^2 + 2X = X(3X + 2)$; also hat f die beiden lokalen Extrema $f(0) = 1$ und $f(-\frac{2}{3}) = \frac{31}{27}$. Da beide Werte grösser als 0 sind, kann f keine weitere reelle Nullstelle haben. Insbesondere liegen die beiden übrigen Nullstellen $b, c \in \mathbb{C}$ von f nicht in $\mathbb{Q}(a)$. Für den Zerfällungskörper $L := \mathbb{Q}(a, b, c)$ von f gilt daher

$$[L/\mathbb{Q}] = [L/\mathbb{Q}(a)] \cdot [\mathbb{Q}(a)/\mathbb{Q}] = 2 \cdot 3 = 6.$$

Über $\mathbb{F}_2$*:* Durch Einsetzen von 0 und 1 sehen wir, dass $f(X) := X^3 + X^2 + 1$ keine Nullstelle in $\mathbb{F}_2$ hat und somit irreduzibel über $\mathbb{F}_2$ ist. Folglich ist

$$L := \mathbb{F}_2[X]/(X^3 + X^2 + 1)$$

ein Stammkörper von f über $\mathbb{F}_2$. Sei $x \in L$ die Restklasse von X. In jedem Körper der Charakteristik 2 ist Quadrieren ein Endomorphismus, insbesondere ist $f(x^2) = f(x)^2 = 0$ in L. Wegen $x \neq 0, 1$ gilt andererseits $x^2 \neq x$. Also hat das kubische Polynom f schon die zwei verschiedenen Nullstellen $x, x^2 \in L$; es zerfällt daher bereits über L in Linearfaktoren. Also ist L schon ein Zerfällungskörper von f über $\mathbb{F}_2$. Wegen der Irreduzibilität folgt schliesslich $[L/\mathbb{F}_2] = 3$.

Aliter: Da x eine Nullstelle von f ist, existiert ein Polynom $g \in L[X]$ vom Grad 2 mit $f(X) = (X - x) \cdot g(X)$. Durch Polynomdivision bestimmen wir dieses zu

$$g(X) = X^2 + (x + 1)X + (x + x^2).$$

Durchprobieren aller 8 Elemente von L gibt uns nun das Element x^2 mit

$$g(x^2) \;=\; x^4 + x^3 + x^2 + x^2 + x \;=\; x(x^3 + x^2 + 1) \;=\; 0.$$

Somit ist x^2 eine weitere Nullstelle von f.

8. Zeige: Für jeden Zerfällungskörper L eines Polynoms vom Grad n über einem Körper K ist der Körpergrad $[L/K]$ ein Teiler von $n!$.

   Lösung: Wir zeigen die Aussage durch Induktion über n. Im Fall $n = 0$ ist $L = K$ und $[L/K] = 1 = 0!$, also gilt die Aussage. Seien nun $f \in K[X]$ ein Polynom vom Grad $n > 0$ und $L = K(\alpha_1, \ldots, \alpha_n)$ ein Zerfällungskörper von f über K.

   Zuerst nehmen wir an, dass f irreduzibel ist in $K[X]$. Dann existiert $c \in K^\times$, so dass cf das Minimalpolynom von α_n über K ist. Mit $K' := K(\alpha_n)$ gilt also $[K'/K] = \deg(cf) = n$. Da α_n eine Nullstelle von f ist, gilt $f(X) = (X - \alpha_n)g(X)$ für ein Polynom $g \in K'[X]$ vom Grad $n - 1$, und nach Konstruktion ist dann $L = K'(\alpha_1, \ldots, \alpha_{n-1})$ ein Zerfällungskörper von g über K'. Nach der Induktionsvoraussetzung ist daher $[L/K']$ ein Teiler von $(n - 1)!$, und somit ist $[L/K] = [L/K'] \cdot [K'/K]$ ein Teiler von $n \cdot (n - 1)! = n!$.

   Ist f hingegen reduzibel, so existieren nicht-konstante Polynome $g, h \in K[X]$ mit $f = gh$. Mit $k := \deg(g)$ gilt dann $\deg(h) = n - k$ und $0 < k < n$. Ohne Beschränkung der Allgemeinheit seien $\alpha_1, \ldots, \alpha_k$ die Nullstellen von g, und $\alpha_{k+1}, \ldots, \alpha_n$ die Nullstellen von h. Dann ist $K' := K(\alpha_1, \ldots, \alpha_k)$ ein Zerfällungskörper von g über K, und L ist ein Zerfällungskörper von h über K'. Nach der Induktionsvoraussetzung ist also $[L/K] = [L/K'] \cdot [K'/K]$ ein Teiler von $k!(n-k)!$. Schliesslich wissen wir, dass der Binomialkoeffizient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ eine ganze Zahl ist. Also ist $k!(n - k)!$ ein Teiler von $n!$, und somit auch $[L/K]$.