Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix
Theresa Kumpitsch

Algebra

Wintersemester 2019/20

Übungsblatt 13 WS 2019/20

Dieses Blatt soll nicht abgegeben werden. Im Tutorium am 11.02. wird Lösung zu Aufgabe 1 sowie Fragen zu den Wiederholungsaufgaben besprochen.

Aufgabe 1. (Resultante)

Sei K ein Körper und seien $f, g \in K[x]$ Polynome von Grad n bzw. m mit

$$\begin{aligned} f &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, \\ g &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0. \end{aligned}$$

Die *Sylvester-Matrix* von f und g ist definiert als $(n+m) \times (n+m)$-Matrix

$$\mathrm{Syl}(f,g) \coloneqq \begin{pmatrix} a_n & a_{n-1} & \cdots & & a_0 & & & \\ & a_n & a_{n-1} & \cdots & & a_0 & & \\ & & \ddots & & & & \ddots & \\ & & & a_n & a_{n-1} & \cdots & & a_0 \\ b_m & b_{m-1} & \cdots & & b_0 & & & \\ & b_m & b_{m-1} & \cdots & & b_0 & & \\ & & \ddots & & & & \ddots & \\ & & & b_m & b_{m-1} & \cdots & & b_0 \end{pmatrix}$$

(a) Betrachten Sie die lineare Abbildung

$$\varphi : \quad K[x]/(g) \times K[x]/(f) \to K[x]/(fg), \quad ([P],[Q]) \mapsto [fP + gQ].$$

Zeigen Sie, dass für eine passende Basiswahl φ gegeben ist durch $\mathrm{Syl}(f,g)^T$.

Die *Resultante von f und g* sei definiert als

$$\mathrm{Res}(f,g) \coloneqq \det(\mathrm{Syl}(f,g)).$$

(b) Zeigen Sie die folgenden Aussagen:

(i) $\mathrm{Res}(f, b_0) = b_0^n$;

(ii) $\mathrm{Res}(f,g) = (-1)^{mn} \cdot \mathrm{Res}(g,f)$;

(iii) Falls $n \leq m$ und Division mit Rest $g = f \cdot h + r$ liefert mit $h, r \in K[x]$, $\deg(r)$ minimal, so gilt:

$$\mathrm{Res}(f,g) = a_n^{m-\deg(r)} \cdot \mathrm{Res}(f,r).$$

(c) Zeigen Sie, dass die Resultante durch die Eigenschaften aus (b) eindeutig bestimmt ist. Folgern Sie daraus: Sind $\alpha_1, \ldots, \alpha_n$ bzw. $\beta_1, \ldots, \beta_m$ die Nullstellen von f, g in einem algebraischen Abschluss $\overline{K}$ von K, so gilt:

$$\begin{aligned}\mathrm{Res}(f,g) &= a_n^m \prod_{i=1}^{n} g(\alpha_i) \\ &= (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\beta_j) \\ &= a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m} (\alpha_i - \beta_j).\end{aligned}$$

(d) Angenommen f ist normiert. Schließen Sie, dass folgender Zusammenhang mit der Diskrimante $\mathrm{Disc}(f)$ von f besteht:

$$\mathrm{Disc}(f) = (-1)^{\binom{n}{2}} \mathrm{Res}(f, f').$$

Wiederholung!

Die folgenden Aufgaben dienen zur Wiederholung und beinhalten zunächst immer einen Teil, in dem wichtige Definitionen, Sätze oder Konzepte eines Themenkomplexes abgefragt werden. Dies soll dabei helfen, sich auf die mündliche Prüfung vorzubereiten. Die folgenden Aufgaben sind einfacher als die bisherigen Übungsaufgaben und sollen auch dabei helfen, das eigene Wissen zu testen. Das Wiederholungsblatt erhebt keinen Anspruch darauf, alle wichtigen Themen/Begriffe vollständig abzudecken oder Prüfungsfragen zu simulieren.

Sei im Folgenden K immer ein Körper.

Aufgabe 2. (Grundlagen Körpererweiterungen)

(a) Wissens-Check:

(i) Was ist eine Körpererweiterung? Wann ist diese endlich bzw. algebraisch?

(ii) Wieso ist die Summe und das Produkt algebraischer Elemente wieder algebraisch?

(iii) Gibt es Körpererweiterungen, die endlich/algebraisch, aber nicht algebraisch/endlich sind?

(iv) Was ist der Grad einer Körpererweiterung? Was sagt der Gradsatz und wie wird dieser bewiesen?

(v) Sei $f \in K[T]$ ein Polynom. Wann ist $K[T]/(f)$ ein Körper? Erklären Sie in diesem Fall den Isomorphismus $K(\alpha) \cong K[T]/(f)$, wobei α eine Nullstelle von f bezeichne.

(vi) Sei α algebraisch über K und sei $f \in K[T]$ ein Polynom mit $f(\alpha) = 0$. In welchem Verhältnis stehen f und $P_{\alpha/K}$? Wann müssen sie gleich sein?

(vii) Wie hängt der Grad des Minimalpolynoms $P_{\alpha/K} \in K[T]$ mit dem Körpergrad der Erweiterung $K(\alpha)/K$ zusammen? Sei nun L/K eine beliebige Erweiterung. Wie hängt $P_{\alpha/K}$ mit den Einbettungen $K(\alpha) \to L$ (sofern solche existieren) zusammen?

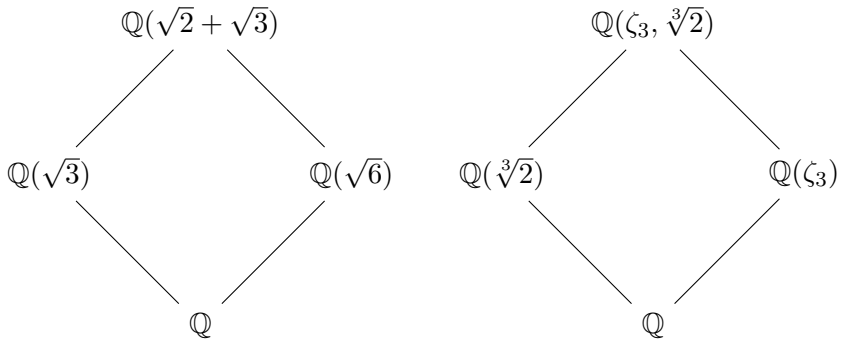
(viii) Nennen Sie ein Beispiel einer Körpererweiterung, die unendlich viele Zwischenerweiterungen besitzt. Kennen Sie eine Bedingung, unter der eine Körpererweiterung nur endlich viele Zwischenkörper hat?

(ix) Wann nennt man einen Körper algebraisch abgeschlossen? Was ist ein algebraische Abschluss eines Körpers? Wieso ziemt es sich nicht, von *dem* algebraischen Abschluss zu sprechen?

(b) Könnens-Check:

(i) Sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Geben Sie eine $\mathbb{Q}$-Basis von K sowie den Grad von $K/\mathbb{Q}$ an. Geben Sie ferner ein primitives Element α an sowie jeweils das Minimalpolynom von α über $\mathbb{Q}$ und $\mathbb{Q}(\sqrt{3})$.

(ii) Bestimmen Sie zu jeder dieser Körpererweiterungen den Grad:



(iii) Es sei $f \in \mathbb{R}[T]$ ein Polynom von Grad 3. Begründen Sie, dass $\mathbb{R}[T]/(f)$ kein Körper ist.

(iv) Sei $K(\alpha)/K$ eine algebraische Erweiterung von ungeradem Grad. Zeigen Sie, dass $K(\alpha) = K(\alpha^2)$.

(v) Es sei L/K eine algebraische Erweiterung. Ist jeder algebraische Abschluss von L auch ein algebraischer Abschluss von K und umgekehrt?

Aufgabe 3. (Irreduzibilitätskriterien)

(a) Wissens-Check:

(i) Welche Kriterien kennen Sie dafür, dass ein Polynom $f \in K[T]$ irreduzibel ist?

(ii) Was ist eine diskrete Bewertung? Geben Sie Beispiele an.

(iii) Sei f ein über $\mathbb{Z}[T]$ irreduzibles Polynom. Ist es dann auch über $\mathbb{Q}[T]$ irreduzibel?

(iv) Skizzieren Sie den Beweis für das Eisensteinkriterium.

(v) Sei $f \in \mathbb{Z}[T]$ und $\overline{f} \in \mathbb{F}_p[T]$ seine Reduktion mod p. Angenommen $\overline{f}$ ist reduzibel/irreduzibel. Gilt dies dann auch für f?

(b) Könnens-Check: Prüfen Sie die folgenden Polynome auf Irreduzibilität.

$$T^2 - 2 \in \mathbb{F}_3[T]; \quad T^3 + 2T + 1 \in \mathbb{Z}[T]; \quad ; T^{2018} + 2017T^{2017} - 2017 \in \mathbb{Z}[T];$$

$$3T^5+14T^3-21T^2+49T-7 \in \mathbb{Z}[T]; \quad T^4-5T^3+2T^2+2T+1 \in \mathbb{Z}[T]; \quad T^4+1 \in \mathbb{Z}[T].$$

Aufgabe 4. (Eigenschaften von Körpererweiterungen: normal und separabel)

(a) Wissens-Check:

(i) Nennen Sie drei (äquivalente) Definitionen einer (endlichen) normalen Körpererweiterungen. Geben Sie Beispiele und Gegenbeispiele an.

(ii) Sei $L/M/K$ ein Körperturm und L/K normal. Ist dann auch M/K bzw. L/M normal?

(iii) Sei K ein Körper und $f \in K[T]$ ein nicht-konstantes Polynom von Grad d. Was können Sie über den Grad des Zerfällungskörpers sagen?

(iv) Was ist die Charakteristik eines Körpers K? Wieso ist diese immer 0 oder eine Primzahl? Sei nun L/K eine Körpererweiterung. Warum hat L die gleiche Charakteristik wie K?

(v) Wann nennt man eine Körpererweiterung separabel? Erklären Sie, warum jede Erweiterung von $\mathbb{Q}$ und jede endliche Erweiterung von $\mathbb{F}_p$ separabel ist.

(vi) Was sagt der Satz vom primitiven Element über endliche separable Körpererweiterungen L/K? Was hat diese Aussage mit der Anzahl von Zwischenkörpern zu tun?

(vii) Skizzieren Sie den Beweis des Satzes vom primitiven Elementen. Erklären Sie inbesondere, wo die beiden Voraussetzungen an L/K eingehen.

(b) Könnens-Check:

(i) Bestimmen Sie zu den folgenden Polynomen jeweils den Zerfällungskörper in $\mathbb{C}$ über $\mathbb{Q}$:

$$T^2 - 3; \quad T^4 - 2T^2 - 2; \quad T^4 - 7; \quad T^5 - 1.$$

(ii) Zeigen Sie, dass die Körpererweiterungen $\mathbb{Q}(i\sqrt{5})/\mathbb{Q}$ und $\mathbb{Q}((i+1)\sqrt[4]{5})/\mathbb{Q}(i\sqrt{5})$ normal sind, jedoch $\mathbb{Q}((i+1)\sqrt[4]{5})/\mathbb{Q}$ nicht.

(iii) Sei K ein Körper der Charakteristik $p > 0$. Zeigen Sie: Ist L/K eine endliche Körpererweiterung mit $p \nmid [L : K]$, so ist L/K separabel.

(iv) Es sei $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. Bestimmen Sie $[L : \mathbb{Q}]$ und $[L : \mathbb{Q}]_s$ und geben Sie alle Homomorphismen $L \to \overline{\mathbb{Q}}$ an.

(v) Zeigen Sie: Ist L/K eine endliche normale Körpererweiterung und $G := \mathrm{Aut}_K(L)$, so ist die Körpererweiterung L/L^G galoissch und $[L : L^G] = [L : K]_s$.

Aufgabe 5. (Theorie endlicher Körper)

(a) Wissens-Check:

(i) Wieso gibt es keinen Körper mit 6 Elementen?

(ii) Wie ist der Frobeniusendomorphismus definiert? Erklären Sie dessen Bedeutung für die Theorie endlicher Körper.

(iii) Sei $K = \mathbb{F}_q$ mit $q = p^r$. Begründen Sie, dass $\#\,\mathrm{Aut}_{\mathbb{F}_p}(K) = r$.

(iv) Erklären Sie, warum jede Erweiterung endlicher Körper normal und separabel ist.

(v) Seien L und K endliche Körper mit $\#L = \#K$. Folgt dann $K \cong L$?

(vi) Wann ist $\mathbb{F}_q$ ein Unterkörper von $\mathbb{F}_{q'}$?

(vii) Skizzieren Sie den Beweis dafür, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist.

(b) Könnens-Check:

(i) Sei $f = T^3 - T + 1 \in \mathbb{F}_3[T]$ und $F = \mathbb{F}_3[T]/(f)$. Geben Sie eine $\mathbb{F}_3$-Basis von F an und bestimmen Sie $\#F$. Bestimmen Sie eine Zerlegung von f in $F[T]$ in irreduzible Faktoren und geben Sie ein erzeugendes Element von $F^\times$ an.

(ii) Zeigen Sie, dass jede Erweiterung endlicher Körper einfach ist.

(iii) Sind die Körpererweiterungen $\mathbb{F}_{81}/\mathbb{F}_9$ und $\mathbb{F}_{25}(t)/\mathbb{F}_{25}(t^8)$ normal?

Aufgabe 6. (Hauptsatz der Galoistheorie)

(a) Wissens-Check:

(i) Wann nennt man eine Körpererweiterung L/K galoissch? Nennen sie drei (äquivalente) Definitionen. Wie ist die Galoisgruppe von L/K? Nennen Sie Beispiele und Gegenbeispiele.

(ii) Sei L/K eine endliche Galoiserweiterung. Erklären Sie, warum $L = K(\alpha)$ für passendes $\alpha \in L$ und nennen Sie den Zusammenhang von $[L : K], \# \operatorname{Gal}(L/K)$ und $\deg(P_{\alpha,K})$.

(iii) Was sagt der Hauptsatz der Galoistheorie über den Zusammenhang zwischen Zwischenkörpern einer Galoiserweiterung L/K und den Untergruppen der Galoisgruppe $\operatorname{Gal}(L/K)$ aus? Was macht diese Korrespondenz mit Inklusionen? Skizzieren Sie den Beweis!

(iv) Sei $L/M/K$ ein Körperturm und L/K galoissch. Erklären Sie, warum L/M immer galoissch ist. Wann ist auch M/K galoisch?

(v) Sei L/K eine Galoiserweiterung mit Galoisgruppe G und $f \in K[T]$ ein irreduzibles Polynom. Beschreiben Sie die Operation von G auf den Nullstellen von f. Welche Eigenschaften hat diese Operation? Warum ist die Irreduzibilität wichtig?

(vi) Definieren sie die Galoisgruppe $\operatorname{Gal}(f)$ eines separablen, nicht-konstanten Polynoms $f \in K[T]$ von Grad n und erklären Sie, wie sich diese als Permutationsgruppe $\operatorname{Gal}(f) \to S_n$ auffassen lässt. Wann handelt es sich um eine transitive Permutationsgruppe?

(b) Könnens-Check:

(i) Angenommen $\operatorname{char}(K) \neq 2$. Zeigen Sie, dass quadratische Erweiterungen von K immer galoissch sind. Geben Sie die Galoisgruppe an.

(ii) Handelt es sich bei den folgenden Erweiterungen um Galoiserweiterungen:

$$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}; \quad \mathbb{F}_{25}/\mathbb{F}_5; \quad \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}; \quad \mathbb{F}_p(t)/\mathbb{F}_p(t^p); \quad \mathbb{Q}(t)/\mathbb{Q}(t^2).$$

(iii) Bestimmen Sie die Galoisgruppe von $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Geben Sie alle Untergruppen und Zwischenkörper an.

(iv) Es sei L/K eine Galoiserweiterung und mit Galoisgruppe G und $\alpha \in L$ mit $\sigma(\alpha) \neq \alpha$ für alle $\mathrm{id} \neq \sigma \in G$. Zeigen Sie, dass $L = K(\alpha)$.

(v) Geben Sie die Galoisgruppe von $T^n - t$ über $\mathbb{C}(t)$ an.

(vi) Zeigen Sie, dass für ein irreduzibles separables Polynom mit abelscher Galoisgruppe gilt $\# \operatorname{Gal}(f) = \deg(f)$.

Aufgabe 7. (Kreisteilungskörper)

(a) Wissens-Check:

(i) Definieren Sie das n-te Kreisteilungspolynom $\Phi_n(T)$ und beweisen Sie, dass $\Phi_n(T) \in \mathbb{Z}(T)$. Was ist der Grad von $\Phi_n(T)$?

(ii) Welche Voraussetzung an die Charakteristik von K muss gestellt werden, damit die Erweiterung $K(\mu_n)/K$ galoissch ist?

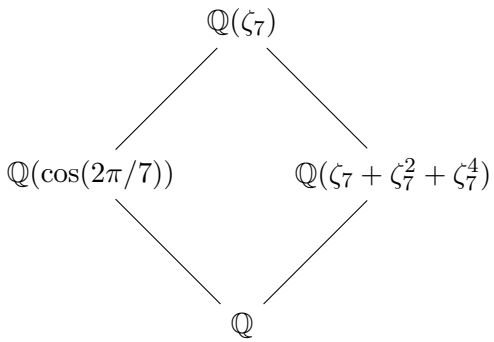
(iii) Beschreiben Sie den zyklotomischen Charakter. Skizzieren Sie, wieso dieser für $K = \mathbb{Q}$ ein Isomorphismus ist. Welche Eigenschaften von $\mathbb{Q}$ gehen in den Beweis ein?

(b) Könnens-Check:

(i) Geben Sie für $n = 1, 2, 3, 4, 5$ das n-te Kreisteilungspolynom $\Phi_n(T)$ an.

(ii) Zeigen Sie, das für teilerfremde Zahlen n, m gilt: $\mathbb{Q}(\zeta_{nm}) = \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m)$.

(iii) Bestimmen Sie zu jeder dieser Zwischenerweiterungen von $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ den Grad und argumentieren Sie, warum es keine weiteren Zwischenkörper geben kann.



(iv) Zeigen Sie, dass es eine Galoiserweiterung $L/\mathbb{Q}$ gibt mit $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

(v) Ist $\zeta = e^{2\pi i/13}$ mit Zirkel und Lineal konstruierbar?

Aufgabe 8. (Sylowsätze und ihre Anwendung, Auflösbarkeit von Gruppen)

(a) Wissens-Check:

(i) Definieren Sie, was eine Sylow-Untergruppe einer endlichen Gruppe G ist. Wann besitzt G eine p-Sylow-Untergruppe?

(ii) Geben Sie die Sylowsätze an. Skizzieren Sie den Beweis! Was sind die wichtigen Ideen und Techniken?

(iii) Wie hängt die Anzahl der p-Sylowgruppen in G mit dem Normalisator einer p-Sylowgruppe in der G zusammen?

(iv) Was sagt der Fundamentalsatz der Algebra und wie hängt dieser mit Sylowgruppen zusammen?

(v) Wann ist eine Zahl mit Zirkel und Lineal konstruierbar? Wie lässt sich dies mit Hilfe von p-Gruppen formulieren?

(vi) Für welche n ist die alternierende Gruppe A_n einfach?

(vii) Erklären Sie, was Subnormalreihen und Kompositionsreihen einer Gruppe sind. Beweisen Sie, dass eine endliche Gruppe eine Kompositionsreihe besitzt. Inwiefern ist diese eindeutig?

(viii) Was können das Zentrum $Z(G)$ und die Kommutatorgruppe $[G, G]$ einer einfachen Gruppe aussagen?

(ix) Wann nennt man eine Gruppe auflösbar? Erklären Sie, warum die Symmetrische Gruppe für $n \geq 5$ nicht auflösbar ist.

(b) Könnens-Check:

(i) Bestimmen Sie bis auf Isomorphie alle Gruppen der Ordnung 99.

(ii) Bestimmen Sie jeweils zu jedem Primteiler der Anzahl der Gruppenelemente eine Sylowgruppe in der angegebenen Gruppe:

$$\mathbb{Z}/4\mathbb{Z}; \quad \mathbb{Z}/100\mathbb{Z}; \quad S_3; \quad \mathbb{Z}/21\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}.$$

(iii) Sei P eine p-Sylowgruppe einer endlichen Gruppe G. Begründen Sie, dass p kein Teiler von $(N_G(P) : P)$ ist.

(iv) Beschreiben Sie alle Normalteiler von A_4 und S_4.

(v) Bestimmen Sie die Kompositionsfaktoren von S_n für alle $n \in \mathbb{N}$.

(vi) Prüfen Sie, ob die folgenden Gruppen aufösbar sind:

$$S_4; \quad S_6 \times \mathbb{Z}/6\mathbb{Z}; \quad S_3 \times S_3.$$

(vii) Seien $p \neq \ell$ Primzahlen. Zeigen Sie, dass eine Gruppe der Ordnung $p\ell$ auflösbar ist.

(viii) Sei L/K eine Galoiserweiterung mit nicht-abelscher Galoisgruppe G mit $\#G = 9 \cdot 13$. Zeigen Sie, dass es 9 Zwischenkörper von Grad 13 über K gubt.

Aufgabe 9. (Radikalerweiterungen und Lösungsformeln)

(a) Wissens-Check:

(i) Angenommen n ist kein Vielfaches von $\mathrm{char}(K)$ und $f = T^n - a \in K[T]$. Sei L/K der Zerfällungskörper von f. Erklären Sie, warum $\mathrm{Gal}(L/K)$ eine auflösbare Gruppe ist.

(ii) Welche (weiteren) Bedingungen muss man an a bzw. K stellen damit f irreduzibel ist?

(iii) Angenommen $\mu_n \subseteq K$. Erklären Sie den Zusammenhang endlicher zyklischer Erweiterungen L/K und (irreduziblen) Polynomen der Form $T^n - a \in K[T]$. Geben Sie in diesem Fall $\mathrm{Gal}(L/K)$ konkret an.

(iv) Angenommen $\mathrm{char}(K) = 0$. Was hat die Auflösbarkeit eines (nicht-konstanten separablen) Polynoms durch Radikale mit der Auflösbarkeit der Galoisgruppe $\mathrm{Gal}(f)$ zu tun? Erklären Sie, wieso der in diesem Zusammenhang entstehende Körperturm sukzessiver Radikalerweiterungen aussieht und was dies mit Kompositionsreihen zu tun hat. Wo benutzen wir dabei die Annahme über die Charakteristik?

(v) Erklären Sie die Relevanz der Erkenntnis, dass S_n für $n \geq 5$ nicht auflösbar ist in diesem Zusammenhang.

(vi) Was sind (elementar-)symmetrische Polynome? Nutzen Sie diese um eine Aussage über den Zusammenhang der Koeffizienten und der Nullstellen eines Polynoms zu machen.

(b) Könnens-Check:

(i) Zeigen Sie, dass wenn eine Nullstelle eines über $\mathbb{Q}$ irreduziblen Polynoms f in einer Radikalerweiterung von $\mathbb{Q}$ liegt, so liegt auch jede andere Nullstelle von f in einer Radikalerweiterung.

(ii) Zeigen Sie, dass ein Polynom $f \in \mathbb{Q}[T]$ mit $\mathrm{Gal}(f) = D_n$ durch Radikale auflösbar ist.

(iii) Es sei L der Zerfällungskörper von $T^7 - 1 \in \mathbb{Q}[T]$. Geben Sie einen Unterkörper von L an, der keine Radikalerweiterung von $\mathbb{Q}$ ist.

(iv) Stellen Sie die folgenden symmetrische Funktionen jeweils explizit durch elementarsymmetrische Polynome dar:

$$X_1^2 + X_2^2 + X_3^2 \in K[X_1, X_2, X_3];$$
$$X_1^4 + X_1^3 X_2 + X_1 X_2^3 + X_2^4 \in K[X_1, X_2];$$
$$X_1^3 + X_2^3 + X_3^3 \in K[X_1, X_2, X_3].$$

Dieses Blatt wird weder abgegeben noch korrigiert, sondern wird im Tutorium besprochen. Downloads von Übungsblättern und Informationen zur Vorlesung unter

`http://www.uni-frankfurt.de/81425887/Algebra`