

Algebra

— Blatt 11 —

(Tutoriumsblatt)

Aufgabe 0 (Vorbereitung auf das Tutorium)

- (a) Wie ist ein Zerfällungskörper eines Polynoms $f \in K[x]$ über einem Körper K definiert? Ist $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ ein Zerfällungskörper von $x^2 - 3$?
- (b) Angenommen, $L|K$ ist eine Körpererweiterung, und $f \in K[x]$ ist ein Polynom mit der Eigenschaft, dass L der Zerfällungskörper von f über K ist. Ist f durch diese Eigenschaft eindeutig bestimmt?
- (c) Durch welche beiden Eigenschaften ist ein algebraischer Abschluss eines Körpers K definiert?
- (d) Warum sind die Elemente eines Körpers K mit p^n Elementen ($n \in \mathbb{N}$, p Primzahl) alle Nullstellen des Polynoms $x^{p^n} - x$?
- (e) Wenn P der Primkörper von K ist, welchen Wert hat der Erweiterungsgrad $[K : P]$? Was kann über die Elementezahl von Teilkörpern des Körpers K ausgesagt werden?

Aufgabe 1

- (a) Bestimmen Sie den Zerfällungskörper $L \subseteq \mathbb{C}$ von $f = x^7 - 5$ über \mathbb{Q} sowie den Grad $[L : \mathbb{Q}]$. Dabei darf ohne Beweis verwendet werden, dass $\zeta = e^{2\pi i/7}$ in \mathbb{C}^\times ein Element der Ordnung 7 ist, dass f über \mathbb{Q} irreduzibel ist und dass $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$ gilt.
- (b) Bestimmen Sie die Anzahl der \mathbb{Q} -Homomorphismen $L \rightarrow \mathbb{R}$, $L \rightarrow \mathbb{Q}(\zeta)$ und $\mathbb{Q}(\sqrt[7]{5}) \rightarrow L$.

Aufgabe 2

Beweisen oder widerlegen Sie die folgenden Aussagen.

- (a) Ist K ein algebraisch abgeschlossener Körper, so gilt $|K| = \infty$.
- (b) Ist K ein Körper mit $|K| = \infty$, dann ist K algebraisch abgeschlossen.
- (c) Ist K ein algebraisch abgeschlossener Körper, dann gibt es keinen Erweiterungskörper L von K mit einem endlichem Erweiterungsgrad $[L : K] > 1$.
- (d) Sei K ein Körper, zu dem es keinen Erweiterungskörper L mit einem endlichem Erweiterungsgrad $[L : K] > 1$ gibt. Dann ist K algebraisch abgeschlossen.

Aufgabe 3

Sei K ein Körper mit $|K| = 7^5$. Wir setzen voraus, dass der Primkörper von K mit \mathbb{F}_p übereinstimmt, für eine geeignete Primzahl p .

- (a) Bestimmen Sie p und $[K : \mathbb{F}_p]$, und begründen Sie Ihre Ergebnisse.
- (b) Entscheiden Sie (mit Begründung), ob das Polynom $x^2 - 3 \in \mathbb{F}_p[x]$ in K eine Nullstelle hat.
- (c) Sei $f \in \mathbb{F}_p[x]$ ein über \mathbb{F}_p irreduzibles Polynom vom Grad 5, das in K eine Nullstelle α besitzt. Zeigen Sie, dass f in $\mathbb{F}_p[x]$ ein Teiler von $x^{7^5} - x$ ist.

Aufgabe 4 (*Zahlentheorie*)

Sei $R = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ der Ring der Gaußschen Zahlen und $N : R \rightarrow \mathbb{N}_0$ die Normfunktion gegeben durch $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$ für $\alpha = a + ib \in R$.

- (a) Begründen Sie, dass jedes Primelement π in R zu genau vier Elementen aus R assoziiert ist.
- (b) Bestimmen Sie bis auf Reihenfolge alle Zerlegungen des Elements $12 + 6i$ in Primelemente. Dabei darf verwendet werden, dass R ein faktorieller Ring ist.
- (c) Zeigen Sie: Ist p eine Primzahl, dann ist entweder p ein Primelement in R , oder es gibt ein Primelement π in R mit $p = \pi\bar{\pi}$.
- (d) Zeigen Sie: Ist $\alpha \in R$ und $N(\alpha)$ Produkt zweier verschiedener Primzahlen, dann ist α kein Primelement in R .

Dieses Blatt wird vom 17. bis zum 20. Januar im Tutorium bearbeitet.

Algebra

— Blatt 11 —

(Globalübungsblatt)

Aufgabe 1 (6+4 Punkte)

Sei K ein Körper, $f \in K[x]$ ein Polynom vom Grad $n \in \mathbb{N}$ und L der Zerfällungskörper von f über K .

- (a) Beweisen Sie die Ungleichung $[L : K] \leq n!$.
- (b) Zeigen Sie: Gilt $[L : K] = n!$, dann ist f irreduzibel über K .
Ist die Umkehrung dieser Aussage allgemein auch richtig?

Aufgabe 2 (2+3+2+3 Punkte)

Bestimmen Sie vom Körper $K = \mathbb{F}_{3^6}$ jeweils die Anzahl

- (a) der Teilkörper,
- (b) der Elemente α mit $K = \mathbb{F}_3(\alpha)$,
- (c) der Untergruppen von K^\times und
- (d) der Elemente α mit $K^\times = \langle \alpha \rangle$.

Aufgabe 3 (3+3+4 Punkte)

Sei p eine Primzahl und $f = x^6 + 1 \in \mathbb{F}_p[x]$. Zeigen Sie:

- (a) Für $p \in \{2, 3\}$ ist f reduzibel in $\mathbb{F}_p[x]$.
- (b) Für $p > 3$ enthält die Gruppe $\mathbb{F}_{p^2}^\times$ ein Element der Ordnung 12.
- (c) Das Polynom f ist reduzibel in $\mathbb{F}_p[x]$.

Hinweis: Für Teil (c) überlegen Sie, welcher Zusammenhang zwischen den Nullstellen von f und den Elementen der Ordnung 12 in $\mathbb{F}_{p^2}^\times$ besteht, und betrachten Sie die Minimalpolynome solcher Elemente.

Aufgabe 4 (Zahlentheorie) (5+5 Punkte)

- (a) Sei R ein faktorieller Ring, K sein Quotientenkörper, und seien $a, b, c \in R \setminus \{0_R\}$. Sei außerdem $d \in R$ ein größter gemeinsamer Teiler von a und b . Zeigen Sie, dass dann cd ein größter gemeinsamer Teiler von ac und bc ist.
- (b) Laut Vorlesung ist der Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen faktoriell. Bestimmen Sie alle größten gemeinsamen Teiler und alle kleinsten gemeinsamen Vielfachen der Elemente $\alpha = 40(1+i)(2+i)$ und $\beta = 180(1-i)$ in $\mathbb{Z}[i]$, möglichst *ohne* den Euklidischen Algorithmus zu verwenden.

Abgabe: Dienstag, 25. Januar 2022, 12:15 Uhr

Verspätete Abgaben können aus organisatorischen Gründen leider nicht nachträglich angenommen werden. Bitte geben Sie auf jeder Abgabe die Nummer Ihrer Übungsgruppe an.