

Modulprüfung Algebra

Bitte ausfüllen:

Name, Vorname	Matrikelnummer	Studiengang

Bitte beachten Sie die folgenden **Hinweise**:

- **Bearbeitungszeit:** 120 Minuten
- **Erlaubte Hilfsmittel:** Der offizielle Spickzettel liegt bei.
- Mobiltelefone müssen während der gesamten Klausur komplett ausgeschaltet und so verstaut sein, dass sie nicht sichtbar sind.
- Bearbeitungen mit Bleistift oder Rotstift sind nicht zulässig!
- Bitte beschriften Sie alle Blätter zur Abgabe mit Ihrem Namen!
- Bei den Kästchenaufgaben reicht es, die Ergebnisse einzutragen.
Ansonsten ist immer eine **Begründung** verlangt.
- Bei der Aufgabe 3 und 5 (b) gibt es für leere Kästchen null Punkte und für falsche Antworten werden **negative Punkte** vergeben.
Die Gesamtpunktzahl der Aufgabe kann allerdings nicht negativ werden.
- Ergebnisse der Klausur gibt es voraussichtlich ab Anfang Oktober.
Die Klausureinsicht findet am 18.10.2010 von 14:00 bis 15:30 im Raum 8.141 statt.

VIEL ERFOLG!

Aufgabe 1 (ca. 2+2 Punkte)

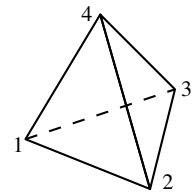
- (a) Zeigen Sie, dass $\sqrt{3}$ irrational ist.
- (b) Die Menge $\mathbb{Q}[\sqrt{3}] = \{ a + b\sqrt{3} : a, b \in \mathbb{Q} \}$ ist ein Teilring von \mathbb{R} .
Ist $\mathbb{Q}[\sqrt{3}]$ ein Körper? Begründen Sie kurz.

Lösungshinweise: —

- (a) Das Polynom $X^2 - 3 \in \mathbb{Z}[X]$ ist nach Eisenstein zu $p = 3$ über \mathbb{Z} irreduzibel und damit nach Gauß auch irreduzibel über \mathbb{Q} . Anders gesagt hat die Gleichung $X^2 = 3$ keine rationale Lösung, also ist $\sqrt{3}$ irrational. Alternativ kann man den üblichen Beweis über die diophantische Gleichung $a^2 = 3b^2$ führen.
- (b) Wir müssen nur zu einem Element $a + b\sqrt{3} \neq 0$ ein Inverses finden. Dies ist gegeben durch $\frac{a-b\sqrt{3}}{a^2-3b^2}$ wie man leicht nachprüft. Dieses Element kann auch so definiert werden, da die Gleichung $a^2 - 3b^2$ im Nenner nur die triviale Lösung $a = b = 0$ besitzt.

Aufgabe 2 (ca. 1+2+2+4+1 Punkte) Symmetriegruppen

Sei T ein regelmäßiges Tetrader im \mathbb{R}^3 wie rechts skizziert und $G < \text{SO}(3, \mathbb{R})$ die Gruppe der orientierungserhaltenden Isometrien (Drehungen) von T .



- (a) Die Gruppe hat Ordnung $|G| = \boxed{}$. *Hinweis:* Bahnengleichung.

- (b) Die Operation von G auf den Ecken ergibt eine Einbettung $G \rightarrow S_4$.

Geben Sie die Elemente der Bildgruppe $H < S_4$ in Zykelschreibweise an.

- (c) Die Gruppe H zerfällt in vier Konjugationsklassen mit 1, 4, 4 und 3 Elementen.

Zählen Sie jede Konjugationsklasse durch Angabe ihrer Elemente auf.

- (d) Geben Sie jeweils eine Untergruppe von H der Ordnung 2, 3, 4, 5, 6 ohne Beweis an oder begründen Sie, warum eine solche Untergruppe nicht existieren kann.

Hinweis: Jede Untergruppe vom Index 2 ist normal.

- (e) Welche der von Ihnen angegebenen Untergruppen sind Sylow-Gruppen von H ?

Lösungshinweise: —

- (a) Es ist $|G| = |G_x| \cdot |Gx|$ für eine Ecke x des Tetraeders. Die Bahn unter der Drehgruppe besteht aus allen 4 Ecken und der Stabilisator aus allen Rotationen, die x festlassen. Davon gibt es genau 3. Die Gruppe hat also 12 Elemente.
- (b)

$id, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)$
--
- (c)

$\{id\}, \{(123), (243), (134), (142)\}, \{(132), (143), (234), (124)\}, \{(12)(34), (13)(24), (14)(23)\}$
--
- (d) $H_1 = \{id\}, H_2 = \{id, (12)(34)\}, H_3 = \{id, (123), (132)\}, H_4 = \{id, (12)(34), (13)(24), (14)(23)\}$. Eine Untergruppe der Ordnung 5 kann es nach Lagrange nicht geben, da 5 kein Teiler von 12 ist. Auch eine Untergruppe der Ordnung 6 ist nicht möglich, da diese normal wäre und somit eine disjunkte Vereinigung von Konjugationsklassen sein müsste. Das Ergebnis in (c) zeigt aber, dass dies nicht möglich ist.
- (e) Sylowgruppen gehören zu maximalen Primpotenzteilern der Gruppenordnung $12 = 3 \cdot 2^2$. Also sind H_3 und H_4 Sylowgruppen. (Je nach Definition ist auch H_1 eine Sylowgruppe zu allen Primzahlen ≥ 5 .)

Aufgabe 3 (ca. 6 Punkte) Zerlegbarkeit in Polynomringen

Sind die folgenden Polynome in den angegebenen Ringen irreduzibel?

(Bitte tragen Sie "red" für reduzibel und "irr" für irreduzibel ein.)

	in $\mathbb{Z}/_2[X]$	in $\mathbb{Z}[X]$	in $\mathbb{R}[X]$	in $\mathbb{C}[X]$
$3X + 3$			irr	
$X^2 + 2X + 5$				red
$X^3 + 9X^2 - 5$			red	red
$X^5 + 6X^3 - 6X^2 + 3$				

Lösungshinweise: —

	in $\mathbb{Z}/_2[X]$	in $\mathbb{Z}[X]$	in $\mathbb{R}[X]$	in $\mathbb{C}[X]$
$3X + 3$	irr	red	irr	irr
$X^2 + 2X + 5$	red	irr	irr	red
$X^3 + 9X^2 - 5$	irr	irr	red	red
$X^5 + 6X^3 - 6X^2 + 3$	red	irr	red	red

Aufgabe 4 (ca. 2+2+5 Punkte) Gruppen

- (a) Bestimmen Sie die Elementarteilerform der Matrix $\begin{pmatrix} 6 & -6 \\ 4 & 0 \end{pmatrix}$.
- (b) Man bestimme alle abelschen Gruppen der Ordnung $2009 = 41 \cdot 49$ bis auf Isomorphie.
- (c) Man bestimme alle Gruppen der Ordnung 2009. (Mit Hilfe der Sylow-Sätze.)

Lösungshinweise: —

- (a) *Elementare Umformungen liefern die Elementarteilerform:*
 $\begin{pmatrix} 6 & -6 \\ 4 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & -6 \\ 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & -6 \\ 0 & 12 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix}$
 Alternativ ist $\text{ggT}(6, -6, 4, 0) = 2$ und $\det\left(\begin{pmatrix} 6 & -6 \\ 4 & 0 \end{pmatrix}\right) = 24$. Damit folgt dieselbe Elementarteilerform.
- (b) *Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen gibt es genau die beiden Möglichkeiten $\mathbb{Z}/_{41} \times \mathbb{Z}/_{49}$ und $\mathbb{Z}/_{41} \times \mathbb{Z}/_7 \times \mathbb{Z}/_7$.*
- (c) *Nach Sylow ist die Anzahl m_{41} der 41-Sylowgruppen ein Teiler von 49 und kongruent $1 \pmod{41}$. Damit muss $m_{41} = 1$ sein. Ebenso ist m_7 ein Teiler von 41 und kongruent zu $1 \pmod{7}$, also $m_7 = 1$. Damit sind beide Sylow-Untergruppen normal in der Gruppe. Diese ist also ein direktes Produkt der beiden Sylowgruppen, die wegen $\text{ggT}(41, 49) = 1$ auch die ganze Gruppe erzeugen. Da jede Gruppe der Ordnung p und p^2 abelsch ist, sind die Sylowgruppen und damit auch unsere Gruppe ebenfalls abelsch und ist damit zu einer der Gruppen in (b) isomorph.*

Aufgabe 5 (ca. 1+4+4 Punkte) Ringe, Ideale, Quotienten

In $\mathbb{Z}[i]$ gilt $i^2 = -1$ und $(1 + i) \cdot (3 - i) + (-i) \cdot (2 - 3i) = 1$.

(a) In $\mathbb{Z}[i]$ gilt $\text{ggT}(1 + i, 2 - 3i) = \boxed{}$.

- (b) Welche der folgenden Isomorphien gelten? **wahr falsch**
- | | | |
|---|--------------------------|--------------------------|
| $\mathbb{Z}[i]/(i) \cong \mathbb{Z}$ | <input type="checkbox"/> | <input type="checkbox"/> |
| $\mathbb{Z}[i]/((1 + i) \cap (2 - 3i)) \cong \mathbb{Z}[i]/(1 + i) \times \mathbb{Z}[i]/(2 - 3i)$ | <input type="checkbox"/> | <input type="checkbox"/> |
| $\mathbb{Z}[i]/(5 - i) \cong \mathbb{Z}[i]/(1 + i) \times \mathbb{Z}[i]/(2 - 3i)$ | <input type="checkbox"/> | <input type="checkbox"/> |
| $\mathbb{Z}[i]/(1 - i) \cong \mathbb{Z}[i]/(1 + i)$ | <input type="checkbox"/> | <input type="checkbox"/> |

- (c) Bestimmen Sie die Anzahl der Elemente in den folgenden Quotientenringen.

$|\mathbb{Z}[i]/(1 + i)| = \boxed{}$, $|\mathbb{Z}[i]/(2 - 3i)| = \boxed{}$

Lösungshinweise: —

- (a) *Nach dem Satz von Bezout ist $\text{ggT}(1 + i, 2 - 3i) = \boxed{1}$ in $\mathbb{Z}[i]$.*
 - (b) **wahr falsch**
- | | | |
|---|-------------------------------------|-------------------------------------|
| $\mathbb{Z}[i]/(i) \cong \mathbb{Z}$ | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| $\mathbb{Z}[i]/((1 + i) \cap (2 - 3i)) \cong \mathbb{Z}[i]/(1 + i) \times \mathbb{Z}[i]/(2 - 3i)$ | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| $\mathbb{Z}[i]/(5 - i) \cong \mathbb{Z}[i]/(1 + i) \times \mathbb{Z}[i]/(2 - 3i)$ | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| $\mathbb{Z}[i]/(1 - i) \cong \mathbb{Z}[i]/(1 + i)$ | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

$$(c) \quad |\mathbb{Z}[i]/(1+i)| = \boxed{2}, \quad |\mathbb{Z}[i]/(2-3i)| = \boxed{13}$$

Aufgabe 6 (ca. 2+1+1 Punkte) Endliche Körper

- (a) Ist das Polynom $P = X^3 - X + 2$ irreduzibel in $\mathbb{F}_5[X]$?
 (b) Konstruieren Sie möglichst explizit einen Körper K mit 125 Elementen.
 (c) Sei L ein Körper mit 625 Elementen. Wie viele Unterkörper hat L ?

Lösungshinweise: —

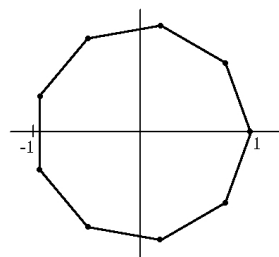
- (a) Es ist $P(0) = 2, P(1) = 2, P(2) = 3, P(3) = 1$ und $P(4) = 2$ in \mathbb{F}_5 . Also hat das Polynom keine Nullstelle in \mathbb{F}_5 und ist damit wegen $\deg(P) = 3$ irreduzibel.
 (b) Da P irreduzibel und \mathbb{F}_5 ein Körper ist, erhalten wir mit $\mathbb{F}_5[X]/(P)$ einen Körper mit $5^{\deg(P)} = 125$ Elementen.
 (c) \mathbb{F}_{p^k} ist genau dann ein Unterkörper von \mathbb{F}_{p^n} , wenn $k \mid n$. In diesem Fall haben wir $n = 4$ und somit insgesamt 3 Unterkörper, entsprechend den Teilern 1, 2 und 4.

Aufgabe 7 (ca. 2+1+2+2+3+1 Punkte) Kreisteilungspolynome

- (a) Wie lautet die Zerlegung von $P = X^9 - 1$ in $\mathbb{Q}[X]$ in irreduzible Polynome?

$$P = \boxed{}$$

- (b) Bestimmen Sie $\xi \in \mathbb{C}$ so, dass $\mathbb{Q}[\xi]$ ein Zerfällungskörper von P über \mathbb{Q} ist.
 (c) Ist $\mathbb{Q}[\xi] : \mathbb{Q}$ eine Galois-Erweiterung?
 (d) Welchen Grad hat die Erweiterung $\mathbb{Q}[\xi]$ über \mathbb{Q} ?
 Bestimmen Sie die Ordnung der Gruppe $\text{Aut}(\mathbb{Q}[\xi] | \mathbb{Q})$.
 (e) Wir betrachten den Automorphismus $\alpha : \mathbb{Q}[\xi] \rightarrow \mathbb{Q}[\xi]$ mit $\alpha(\xi) = \xi^2$. Bestimmen Sie die Ordnung von α .
 (f) Warum lässt sich das regelmäßige 9-Eck nicht mit Zirkel und Lineal konstruieren?


Lösungshinweise: —

- (a) Die Zerlegung in zyklotomische (und damit irreduzible) Polynome ist:

$$P = \boxed{(X-1)(X^2+X+1)(X^6+X^3+1)}$$

- (b) Wenn man eine der 6 primitiven Einheitswurzeln wählt, kann man alle anderen Nullstellen als Potenzen davon erzeugen. Also geht zum Beispiel $\xi = e^{2\pi i/9}$.
- (c) Als Zerfällungskörper ist die Erweiterung normal und weil die Charakteristik von \mathbb{Q} null ist, ist die Erweiterung separabel. (Man sieht es aber auch direkt an den 9 verschiedenen Nullstellen des Polynoms).
- (d) Der Grad stimmt bei einfachen Erweiterungen mit dem Grad des Minimalpolynoms überein. Ist hier also 6. Da es sich um eine Galois-Erweiterung handelt, erhalten wir $|\text{Aut}(\mathbb{Q}[\xi] | \mathbb{Q})| = |\mathbb{Q}[\xi] : \mathbb{Q}| = 6$.
- (e) Es ist $\alpha^2(\xi) = \alpha(\xi^2) = (\alpha(\xi))^2 = \xi^4$ und ebenso $\alpha^3(\xi) = \xi^8, \alpha^4(\xi) = \xi^{16} = \xi^7, \alpha^5(\xi) = \xi^{14} = \xi^5, \alpha^6(\xi) = \xi^{10} = \xi$. Damit ist $\alpha^6 = \text{id}$ und $\alpha^k \neq \text{id}$ für $1 \leq k \leq 5$. Also ist die Ordnung 6. Damit erzeugt α die Galoisgruppe von $\mathbb{Q}[\xi] : \mathbb{Q}$.
- (f) Um das regelmäßige Neuneck zu konstruieren, müssten wir ξ konstruieren können. Das geht aber nur, wenn der Grad der Körpererweiterung eine Zweierpotenz ist. Dies ist hier nicht der Fall, also ist ξ und damit auch das regelmäßige Neuneck nicht mit Zirkel und Lineal konstruierbar.
-