Prof. Dr. Bernd Siebert

Klausur

Algebra
SS 2014

Bearbeitungszeit: 120 Minuten

Nachname: ____________________

Vorname: ____________________

Matrikelnr: ____________________

Es dürfen alle Vorlesungsunterlagen inklusive Übungsaufgaben und Lösungen verwendet werden. Untersagt ist jedoch die Benutzung von Büchern, eines Taschenrechners und anderer elektronischer Geräte. Jede zusätzliche beschriebene Seite muss mit Namen und Matrikelnummer beschriftet werden.

von den Korrektoren auszufüllen:

____

Note nach Klausurpunkten

1	2	3	4	5	6	7	8	9	10

$\sum$:

1. Sei $G = \mathbb{Z}/20$ und H die Untergruppe $\langle [4] \rangle$.

   a) Bestimme die Anzahl der Linksnebenklassen von H in G.

   b) Finde die Ordnung des Elementes $[6] + H$ im Quotienten G/H.

   c) Ist der Quotient G/H zyklisch? Begründe!

(6 Punkte)

Lösung:

a) Es gilt $H = \{[0], [4], [8], [12], [16]\}$. Damit folgt

$$[G : H] = \frac{|G|}{|H|} = \frac{20}{5} = 4.$$

Demnach gibt es 4 Linksnebenklassen von H in G.
Diese sind

$$\begin{aligned}
[0] + H &= \{[0], [4], [8], [12], [16]\} \\
[1] + H &= \{[1], [5], [9], [13], [17]\} \\
[2] + H &= \{[2], [6], [10], [14], [18]\} \\
[3] + H &= \{[3], [7], [11], [15], [19]\}.
\end{aligned}$$

(Diese Liste war nicht gefragt.)

b) Die Ordnung von $x = [6] + H = [2] + H$ in G/H ist die kleinste positive natürliche Zahl n mit $nx = H$. Offenbar ist $x \notin H$ und

$$x + x = ([2] + H) + ([2] + H) = [4] + H = H.$$

Die Ordnung von $[6] + H$ ist demnach 2.

c) Der Quotient G/H ist zyklisch, weil der Quotient einer zyklischen Gruppe wieder zyklisch ist.

2. Sei $G \cong \mathbb{Z}^2 \times (\mathbb{Z}/5)^2 \times \mathbb{Z}/2 \times (\mathbb{Z}/7)^3$. Bestimme ganze Zahlen $d_1, d_2, ..., d_n$ mit $d_i | d_{i+1}$ für $i = 1, ..., n-1$, so dass $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$ gilt.

(4 Punkte)

Lösung:

$$
\begin{aligned}
G &\cong (\mathbb{Z}/5)^2 \times \mathbb{Z}/2 \times (\mathbb{Z}/7)^3 \times \mathbb{Z}^2 \\
&\cong \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/2 \times \mathbb{Z}/7 \times \mathbb{Z}/7 \times \mathbb{Z}/7 \times \mathbb{Z} \times \mathbb{Z} \\
&\cong \mathbb{Z}/7 \times \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/2 \times \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z} \times \mathbb{Z} \\
&\cong \mathbb{Z}/7 \times \mathbb{Z}/5 \cdot 7 \times \mathbb{Z}/2 \cdot 5 \cdot 7 \times \mathbb{Z} \times \mathbb{Z} \\
&\cong \mathbb{Z}/7 \times \mathbb{Z}/35 \times \mathbb{Z}/70 \times \mathbb{Z} \times \mathbb{Z}
\end{aligned}
$$

Demnach gilt $d_1 = 7, d_2 = 35, d_3 = 70, d_4 = 0, d_5 = 0$.

3. Zeige: $\langle (12), (345) \rangle \subset S_5$ ist nicht normal.

(4 Punkte)

Lösung:
Die Zykel (12) und (345) vertauschen und erzeugen demnach eine Gruppe des Isomorphietyp $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Man rechnet $(23)(345)(23) = (245)$ und dieser Dreizykel ist nicht in dem Faktor der Ordung drei der von $(12), (345)$ erzeugten Gruppe enthalten, da sein Träger nicht $\{3, 4, 5\}$ ist.

4. Sei G eine Gruppe der Ordnung $351 = 27 \cdot 13$. Zeige: G hat eine nichttriviale normale Untergruppe.
Hinweis: Betrachte die Anzahl der Sylow Untergruppen.

(4 Punkte)

Lösung:
Die in der Gruppenordnung auftretenden Primzahlen sind 3 und 13. Nach den Sylowsätzen gilt $n_{13} \equiv 1 \mod 13$ und n_{13} teilt 27. Also $n_{13} = 1$ oder $n_{13} = 27$. Ist $n_{13} = 1$ so ist die 13-Sylowgruppe normal. Im Fall $n_{13} = 27$ gibt es, da jede 13-Sylowgruppe prime Ordnung hat und sich diese Gruppen nur trivial schneiden, $27 \cdot 12$ Elemente der Ordnung 13. Es bleiben 27 Elemente, die die 3-Sylowgruppen bilden. Hier hat jede 3-Sylowgruppe die Ordnung 27, also folgt $n_3 = 1$. In jedem Fall hat G eine normale Untergruppe.

5. Sei A ein kommutativer Ring, $\mathfrak{m} \neq A$ ein Ideal, so dass alle $x \in A \backslash \mathfrak{m}$ Einheiten sind. Zeige: A besitzt genau ein maximales Ideal und dieses ist durch $\mathfrak{m}$ gegeben.

(4 Punkte)

Lösung:
$\mathfrak{m}$ ist maximal, da jedes Ideal, das $\mathfrak{m}$ echt enthält, eine Einheit enthält, also gleich A ist. Jedes nicht in $\mathfrak{m}$ enthaltene Ideal enthält nach Voraussetzung eine Einheit, ist also gleich A und somit nicht maximal. Insgesamt ist $\mathfrak{m}$ das einzige maximale Ideal von A.

6. Sei R ein kommutativer Ring. Ein Element $r \in R$ heißt *nilpotent*, falls es ein $n \in \mathbb{N}\backslash\{0\}$ gibt mit $r^n = 0$.

   a) Zeige: $N := \{r \in R : r \text{ ist nilpotent}\}$ ist ein Ideal.

   b) Zeige weiterhin, dass N im Schnitt aller Primideale von R enthalten ist.

(5 Punkte)

Lösung:

a) Sei $a, b \in N$ und $r \in R$. Dann ist $a^n = 0$ und $b^n = 0$ für $m, n \in \mathbb{N} \setminus 0$. Nach dem Binominalsatz gilt

$$(a-b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i (-b)^{m+n-i},$$

für alle $i \in \{1, \cdots, m+n\}$ ist also $i \geq n$ oder $m+n-i \geq m$, also entweder $a^i = 0$ oder $b^{m+n-i} = 0$. Insgesamt also $(a-b)^{m+n} = 0$ und somit ist $a - b \in N$. Das N unter Multiplikation mit R abgeschlossen ist folgt aus $(ra)^n = r^n a^n = 0$. Damit folgt dann auch, dass für $a \in N$" $-a = -1a$ und 0 in N liegen.

b) Sei $N' = \bigcap_{\mathfrak{p} \in R, \mathfrak{p} \text{ prime}} \mathfrak{p}$. Ist $a \in N$ so gilt $a^n = 0 \in \mathfrak{p}$ und demnach ist a^n in jedem Primideal p von R enthalten. Also ist auch $a \in N'$.

7. Zeige: Das Ideal $(X^2 - Y^2) \subset \mathbb{R}[X, Y]$ ist kein Primideal.

(3 Punkte)

Lösung:
Sei $f = X^2 - Y^2 = (X-Y)(X+Y)$. Keiner der beiden Faktoren liegt in (f), denn keines der beiden Ideale $(X-Y)$ und $(X+Y)$ liegt in (f). Aus $a \neq 0$ und $a \in (f)$ folgt nämlich $\deg a \geq 2$: Es gilt $a = f \cdot r$, $r \neq 0$ und somit $\deg a = \deg f + \deg r$, weil $\mathbb{R}$ ein Körper ist. Es folgt $\deg a \geq \deg f = 2$.

8. Sei $f = 2X^{10} - 25X^3 + 10X^2 - 30 \in \mathbb{Q}[X]$. Zeige: $\mathbb{Q}[X]/(f)$ ist ein Körper.

(3 Punkte)

Lösung:
f ist irreduzibel nach Eisenstein. Da $\mathbb{Q}[X]$ ein Hauptidealring ist folgt, dass das Ideal (f) maximal ist, also ist $\mathbb{Q}[X]/(f)$ ein Körper.

9. Sei $F = \mathbb{Q}(\sqrt[8]{2}, i)$. Zeige: $[F : \mathbb{Q}] = 16$.

(4 Punkte)

Lösung:
Nach Eisenstein ist $X^8 - 2$ irreduzibel über $\mathbb{Q}$, also gilt $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 8$. Diese Körpererweiterung ist reell, also hat $X^2 + 1$ keine Nullstellen in $\mathbb{Q}(\sqrt[8]{2})$ und ist als Polynom vom Grad 2, somit über diesen Körper irreduzibel. Die komplexen Nullstellen sind $i, -i$. Insgesamt folgt $[\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}(\sqrt[8]{2})][\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}] = 16$.

10. Sei $\alpha \in \mathbb{C}$ eine Nullstelle des irreduziblen Polynoms $f = X^3 - 3X - 1 \in \mathbb{Q}[X]$. Sei $F = \mathbb{Q}(\alpha)$. Zeige: Es gibt ein $\sigma \in \mathrm{Aut}(F/\mathbb{Q})$ mit $\sigma(\alpha) = 2 - \alpha^2$. (Wenn Sätze der Vorlesung benutzt werden, gib die genaue Referenz an.)

(6 Punkte)

Lösung:
Da die Automorphismen von F über $\mathbb{Q}$ nur durch Permutation der Nullstellen der Minimalpolynome von Elementen von F operiert, müssen wir zunächst überprüfen, dass $2 - \alpha^2$ ebenfalls eine Nullstelle von F ist. In der Tat folgt aus $f(\alpha) = 0$ in F die Relation

$$\alpha^3 = 3\alpha + 1.$$

Man rechnet weiter $\alpha^3 = 3\alpha + 1$, also $\alpha^4 = 3\alpha^2 + \alpha$ und $\alpha^6 = 3\alpha^4 + \alpha^3 = 3(3\alpha^2 + \alpha) + 3\alpha + 1 = 9\alpha^2 + 6\alpha + 1$. Mit dieser Vorbereitung folgt

$$\begin{aligned}
f(2 - \alpha^2) &= (2 - \alpha^2)^3 - 3(2 - \alpha^2) - 1 \\
&= 8 - 12\alpha^2 + 6\alpha^4 - \alpha^6 - 3(2 - \alpha^2) - 1 \\
&= 1 - 9\alpha^2 + 6\alpha^4 - \alpha^6 \\
&= (6 - 6)\alpha + (-9 + 18 - 9)\alpha^2 = 0.
\end{aligned}$$

Da $2 - \alpha^2 \neq \alpha$ haben wir also zwei verschiedene Nullstellen von f in $\mathbb{Q}(\alpha)$ gefunden. Wegen $\deg f = 3$ zerfällt demnach f in $\mathbb{Q}(\alpha)$ in Linearfaktoren. Also ist $\mathbb{Q}(\alpha)$ der Zerfällungskörper von $f \in \mathbb{Q}[X]$ und ist also wegen $\mathrm{char}\, \mathbb{Q} = 0$ eine Galoiserweiterung von $\mathbb{Q}$. Benutze schließlich, dass $\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$ transitiv auf den Nullstellen von $f = \mathrm{Irr}(\alpha, \mathbb{Q})$ operiert, um σ zu finden.

Den letzten Schritt kann man expliziter und etwas einfacher auch durch direkte Anwendung von Satz 17.4 aus der Vorlesung ersetzen mit $K = \mathbb{Q}$, $L = M = \mathbb{Q}(\alpha)$. Der Satz liefert in der Tat ein $\sigma \in \mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$, der die Nullstelle α von $f = \mathrm{Irr}(\alpha, \mathbb{Q})$ auf die Nullstelle $2 - \alpha^2$ von f abbildet.