Karlsruher Institut für Technologie

Institut für Algebra und Geometrie

05. September 2013

Klausur zur Vorlesung

Einführung in Algebra und Zahlentheorie

Name, Vorname:	
Matrikelnummer:	
Fachrichtung:	Semester:

Zur Bearbeitung: Verwenden Sie für die Bearbeitung jeder Aufgabe ein neues Blatt, auf welches Sie die **Nummer der Aufgabe** sowie **Ihren Namen** schreiben.
Führen Sie die Beweise in allen Einzelheiten aus. Wenn Sie Sätze der Vorlesung anwenden, zitieren Sie die Sätze genau. Wo gerechnet werden muss, schreiben Sie nicht nur die Zahlen hin, sondern erklären und begründen Sie alles, was Sie tun.
Zur Auswertung: „Bestanden“ haben Sie die Prüfung sicher, wenn Sie 22 oder mehr der 60 erreichbaren Punkte erzielen.

Punkte (Wird von den Prüfern ausgefüllt!)						Σ	**Note**
1	2	3	4	5	6		
						$\Longleftarrow$	Bitte kreuzen Sie **hier** an, welche Aufgaben Sie bearbeitet haben.

Aufgabe 1 (10 Punkte)

a) Stellen Sie 1 mit Hilfe des euklidischen Algorithmus als ganzzahlige Linearkombination von 18 und 59 dar.

b) Finden Sie alle $x \in \mathbb{Z}$ mit

- $x \equiv 6$ modulo 7,
- $x \equiv 5$ modulo 11 und
- $x \equiv 12$ modulo 59.

Lösung:

a)

$$\begin{aligned} 59 &= 3 \cdot 18 + 5 \\ 18 &= 3 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

Das führt auf

$$1 = 3-1\cdot 2 = 3-(5\cdot 3) = 2\cdot 3-5 = 2\cdot(18-3\cdot 5)-5 = 2\cdot 18-7\cdot 5 = 2\cdot 18-7\cdot(59-3\cdot 18) = 23\cdot 18-7\cdot 59,$$

was auch durch Nachrechnen bestätigt wird.

b) Nach der ersten Kongruenz ist jedes x, das alle 3 Kongruenzen erfüllt, von der Form $x = 7k + 6$ für ein $k \in \mathbb{Z}$.

Nach der zweiten Kongruenz ist dann

$$7k + 6 \equiv 5 \bmod 11.$$

Das ist äquivalent zu

$$7k \equiv 10 \bmod 11$$

und nach Multiplikation mit 8 zu

$$k \equiv 3 \bmod 11.$$

x ist also von der Form $x = 7 \cdot (11l + 3) + 6 = 77l + 27$ für ein $l \in \mathbb{Z}$.

Die dritte Kongruenz liefert schließlich

$$77l + 27 \equiv 12 \bmod 59$$

beziehungsweise

$$18l \equiv -15 \bmod 59.$$

Nach a) ist $23 \cdot 18 \equiv 1 \bmod 59$, also ist

$$l \equiv -345 \equiv 9 \bmod 59.$$

Also sind alle Lösungen der 3 Kongruenzen von der Form $x = 77(59m + 9) + 27 = 4543m + 720$ $(*)$ für ein $m \in \mathbb{Z}$.
Umgekehrt zeigen diese Rechnungen, dass jedes x der Form $(*)$ alle 3 Kongruenzen erfüllt.

Aufgabe 2 (10 Punkte)

a) Zeigen Sie, dass es unendlich viele Primzahlen p des Typs $p \equiv 2$ modulo 3 gibt.

b) Sei $p \equiv 2$ modulo 3 eine Primzahl. Zeigen Sie, dass die Abbildung $f\colon \mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto x^3$ injektiv ist.

c) Sei nun $a \in \mathbb{Z}$. Zeigen Sie, dass es unendlich viele Primzahlen p gibt, so dass die Restklasse von a eine dritte Potenz in $\mathbb{Z}/p\mathbb{Z}$ ist.

Lösung

a) Für die natürliche Zahl $N \geq 3$ setzen wir

$$M := N! - 1.$$

Da 3 ein Teiler von $N!$ ist, ist $M \equiv 2 \pmod 3$.
Die Primteiler von M sind also alle von 3 verschieden, es können aber auch nicht alle bei Division durch 3 Rest 1 lassen, da M ja ihr Produkt ist und dann ebenfalls 1 modulo 3 sein müsste. Außerdem ist jeder Primteiler von M sicher $\geq N$, da er sonst auch $N!$ teilen würde und daher auch $M - N! = -1$.

Es gibt also für jede natürlich Zahl N eine Primzahl, die größer ist als N und bei Division durch 3 Rest 2 lässt.

b) Sei $p \equiv 2 \pmod 3$.

Das Urbild der 0 enthält nur die 0, da $\mathbb{F}_p$ ein Körper und damit nullteilerfrei ist.

Die Einschränkung von f auf $\mathbb{F}_p \setminus \{0\} = \mathbb{F}_p^\times$ ist ein Gruppenendomorphismus der Einheitengruppe. Diese hat $p - 1 \equiv 1 \pmod 3$ Elemente.
Ein nichttriviales Element im Kern von $f|_{\mathbb{F}_p^\times}$ hätte Ordnung 3, kann also nach dem Satz von Lagrange nicht existieren. Damit enthält der Kern nur die 1, und der Homomorphismus ist injektiv.

Zusammen ergibt das die Injektivität von f.

c) Die Aussage stimmt, da es wegen Teil a) unendlich viele Primzahlen $\equiv 2 \pmod 3$ gibt.
Wegen Teil b) ist für jede dieser Primzahlen die Restklasse von a eine dritte Potenz, denn die dort definierte Abbildung f ist als injektive Selbstabbildung einer endlichen Menge auch surjektiv.

Aufgabe 3 (10 Punkte)

a) Sei G eine endliche Gruppe und p eine Primzahl, so dass G genau 140 p-Sylowgruppen enthält. Was ist p?

b) Wieso hat jede 3-Sylowgruppe in S_7 einen Fixpunkt bei der natürlichen Operation auf $\{1, 2, 3, 4, 5, 6, 7\}$?

c) Geben Sie eine 3-Sylowgruppe D in der symmetrischen Gruppe S_7 an.

d) Wieso ist jede 3-Sylowgruppe in S_7 zu D isomorph?

e) Wie viele 3-Sylowgruppen enthält S_7? Wie groß ist der Normalisator $\{g \in G : gDg^{-1} = D\}$ von D in S_7?

Hinweis: Die Teilaufgabe a) hat nur indirekt mit den anderen Teilen zu tun.

Lösung:

a) Nach den Sylowsätzen ist die Anzahl der p-Sylowgruppen kongruent zu 1 modulo p. Es muss also in der Aufgabe p ein Teiler von $140 - 1 = 139$ sein, aber 139 ist selbst eine Primzahl. Daher ist $p = 139$.

b) $\#S_7 = 7!$ wird von 9, aber nicht von 27 geteilt, eine 3-Sylowgruppe hat also 9 Elemente. Wenn solch eine Gruppe auf einer Menge operiert, hat nach der Bahnbilanzformel jede Bahn die Länge 1, 3 oder 9.

Daher muss in der Aufgabe mindestens eine Bahn Länge 1 haben, da 7 sich nicht ganzzahlig aus 3 und 9 darstellen lässt. So eine Bahn besteht aus einem Fixpunkt.

c) Da es keine 9-Zykel in S_7 gibt, hat jedes nichttriviale Element in D Ordnung 3. Die beiden Dreizykel (1 2 3) und (4 5 6) kommutieren miteinander, und erzeugen daher eine Gruppe D mit 9 Elementen.

d) Nach den Sylowsätzen sind je zwei 3-Sylowgruppen zueinander konjugiert und damit insbesondere isomorph, da die Konjugation immer ein Isomorphismus ist.

e) Jede 3-Sylowgrupe wird von zwei kommutierenden Dreizykeln wie in Teil c) erzeugt. Man erhält also für jede Wahl zweier disjunkter 3-elementiger Mengen in $\{1, 2, \ldots, 7\}$ eine 3-Sylowgruppe. Es gibt

$$\binom{7}{3} \cdot \binom{4}{3} = 7 \cdot 5 \cdot 4 = 140$$

Wahlen für zwei solche Mengen. Da aber die Reihenfolge der Wahlen der beiden Mengen keine Rolle spielt, ist die Anzahl der 3-Sylowgruppen nicht 140 (sonst wäre 3=139) sondern 70.

S_7 operiert durch Konjugation transitiv auf der Menge aller 3-Sylowgruppen. Der Normalisator von D ist dann der Stabilisator von D unter dieser Konjugation. Mit der Bahnbilanzformel sehen wir, dass der Normalisator Index 70 in S_7 hat, er besteht also selbst aus

$$\frac{7!}{70} = 72$$

Elementen.

Aufgabe 4 (10 Punkte)
Sei K ein Körper. Gegeben sei der Ring

$$A := \left\{ \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} : a, b, c \in K \right\} \subseteq K^{3\times 3}.$$

Zeigen Sie die nachfolgenden Aussagen:

a) A ist kommutativ.

b) A und $K[X]/(X^3)$ sind als Ringe isomorph.

c) $K[X]/(X^3)$ enthält einen Teilring, der isomorph zu $K[X]/(X^2)$ ist.

Lösung:

a) Seien $a, b, c, d, e, f \in K$ beliebig. Dann ist

$$\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \cdot \begin{pmatrix} d & e & f \\ 0 & d & e \\ 0 & 0 & d \end{pmatrix} = \begin{pmatrix} ad & ae+bd & af+be+cd \\ 0 & ad & ae+bd \\ 0 & 0 & ad \end{pmatrix} = \begin{pmatrix} d & e & f \\ 0 & d & e \\ 0 & 0 & d \end{pmatrix} \cdot \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix}.$$

b) Da A kommutativ ist, können wir die UAE des Polynomrings ausnutzen.
(*Zur Erinnerung:* Sind ein Ringhomomorphismus $\varphi\colon K \to A$ und ein Bild E von X in A gegeben, so gibt es genau einen Ringhomomorphismus $\varphi\colon K[X] \to A$.
Dieser berechnet sich aus $\varphi(a + bX + cX^2 + ...) = \varphi(a) + \varphi(b) \cdot E + \varphi(c) \cdot E^2 + ...)$

Die Abbildung $K \mapsto A$, $r \mapsto r \cdot I_3 = \begin{pmatrix} r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{pmatrix}$ ist natürlich ein Ringhomomorphismus.

Desweiteren ordnen wir X die Matrix $E := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ zu.

Es ist $E^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ und $E^n = 0$ für alle $n \geq 3$.

Also bekommen wir einen Ringhomomorphismus von $K[X] \to A$, gegeben durch

$$\varphi(a + bX + cX^2 + \sum_{i=3}^{<\infty} a_i X^i) = a \cdot I_3 + b \cdot E + c \cdot E^2 = \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix}.$$

An dieser Form sehen wir, dass der Ringhomomorphismus surjektiv ist und dass $f \in K[X]$ genau dann im Kern liegt, wenn $a = b = c = 0$, wenn also f ein Vielfaches von X^3 ist.
Also ist $\text{Kern}(\varphi) = X^3$ und die Aussage folgt mit dem Homomorphiesatz.

c) Wir suchen einen solchen Ring in A und finden die Teilmenge

$$A := \{ \begin{pmatrix} a & 0 & c \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \mid a, b, c \in K \}.$$

Diese ist multiplikativ abgeschlossen (nachrechnen), offensichtlich auch additiv abgeschlossen und enthält 1 und -1 und ist damit ein Teilring von A.

Wie in b) sehen wir, dass $X \mapsto E' = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ einen surjektiven Ringhomomorphismus $\varphi' \colon K[X] \to A'$ induziert. Wegen $E'^2 = 0$ ist $\operatorname{Kern}(\varphi') = X^2$, also $A' \cong K[X]/(X^2)$.

Nachtrag: In b) können wir die Abbildung auch direkt angeben: Hier muss auf jeden Fall gezeigt werden, dass die gegebene Abbildung ein Ringhomomorphismus ist. Anwenden der UAE schenkt uns dieses. Auch in c) können wir einen Teilring R direkt in $K[X]/(X^3)$ angeben und die Bedingungen nachrechnen: Der Homomorphismus aus b) zeigt uns, dass unser Beispiel von oben der Teilring

$$R \coloneqq \{a + cX^2 + (X^3), a, c \in K\} \subseteq K[X]/(X^3)$$

ist. Dann müssen wir noch zeigen, dass die Abbildung zwischen R und $K[X]/(X^2)$, gegeben über

$$a + cX^2 + (X^3) \mapsto a + cX + (X^2)$$

ein Isomorphismus ist.

Aufgabe 5 (10 Punkte)
Sei $f := X^2 + 1 \in \mathbb{F}_3[X]$. Zeigen Sie:

a) $K := \mathbb{F}_3[X]/(f)$ ist ein Körper mit 9 Elementen.

b) Die Restklasse von $X + 1$ erzeugt die Einheitengruppe $K^\times$.

c) Geben Sie alle Erzeuger der Einheitengruppe an.

Lösung:

a) In der Vorlesung haben wir gesehen, dass $K = \mathbb{F}_3[X]/(f)$ ein Körper ist, wenn f irreduzibel ist. Als Polynom vom Grad 3 ist f genau dann reduzibel, wenn es eine Nullstelle hat – Einsetzen der drei Elemente 0, 1, 2 von $\mathbb{F}_3$ zeigt, dass f keine Nullstelle hat. Also ist f irreduzibel, also ist K ein Körper.

Modulo $f = X^2 + 1$ können wir alle Monome größer 2 durch kleinere Monome ausdrücken, denn es ist $\overline{X^2 + 1} = \overline{0}$, also $\overline{X^2} = \overline{-1} = \overline{2}$.
Polynome vom Grad kleinergleich 1 sind genau dann äquivalent, wenn sie gleich sind. Also sind die Polynome $0, 1, 2, X, X + 1, X + 2, 2X, 2X + 1, 2X + 2$ vom Grad kleinergleich 1 ein Vertretersystem der Elemente: Das sind 9 Stück.

(**Allgemein** haben wir in der Vorlesung gesehen, dass für einen Körper L und $g \in L[X]$ irreduzibel, der Körper $L/(g)$ genau $\#L^{\mathrm{grad}(g)}$ viele Elemente hat – das geht mit der gleichen Begründung wie oben und damit ist $\#K = 9$ natürlich auch klar.)

b) Die Einheitengruppe des Körpers besitzt Ordnung $9 - 1 = 8$ Elemente. Diese haben nach Lagrange die (multiplikative) Ordnung 1 (nur das Neutralelement $\overline{1}$), 2, 4 oder 8 (das sind die Erzeuger).
Für ein Element $g \in K^\times$ gilt dann:
g erzeugt $K^\times \Leftrightarrow \mathrm{ord}(g) = 8 \Leftrightarrow \mathrm{ord}(g) \notin \{1, 2, 4\} \Leftrightarrow g^4 \neq \overline{1}$. $(*)$
Speziell für $\overline{X + 1}$ gilt:
$\overline{X + 1}^4 = \overline{X^2 + 2X + 1}^2 = \overline{2X}^2 = \overline{4X^2} = \overline{X^2} = \overline{2} \neq \overline{1}$.

(Stur nachrechnen geht natürlich auch:
$\overline{X + 1} \neq \overline{1}$,
$\overline{X + 1}^2 = \overline{X^2 + 2X + 1} = \overline{2X} \neq \overline{1}$,
$\overline{X + 1}^4 = (\overline{X + 1}^2)^2 = \overline{2X}^2 = \overline{4X^2} = \overline{2} \neq \overline{1}$,
$\overline{X + 1}^8 = (\overline{X + 1}^4)^2 = \overline{2}^2 = \overline{1}$.)

c) **Vorüberlegung:** $K^\times$ ist als zyklische Gruppe isomorph zu $\mathbb{Z}/8\mathbb{Z}$, hat also $\varphi(8) = 4$ Erzeuger.
(φ ist die eulersche φ-Funktion. Oder wir zählen die Erzeuger $1, 3, 5, 7$ einfach.)
Es reicht mit $(*)$ die vier Elemente mit Ordnung 8 zu finden ODER die vier Elemente, die nicht Ordnung 8 haben. (**Bemerkung am Rand:** Diese haben Ordnung 1, 2 und zweimal 4. Das sehen wir in $\mathbb{Z}/8\mathbb{Z}$ ganz schnell.)

NICHT Ordnung 8 haben sicher $\overline{1}$ (Ordnung 1), $\overline{-1} = \overline{2}$ (Ordnung 2). Außerdem hat nach b) $\overline{X + 1}^2 = \overline{2X}$ Ordnung 4 und damit auch $-\overline{X + 1}^2 = \overline{X}$ eine Ordnung ≤ 4.
Also sind die anderen Elemente $\overline{X + 1}, \overline{2X + 2}, \overline{2X + 1}, \overline{X + 2}$ die Erzeuger der Gruppe.

Aufgabe 6 (10 Punkte)
Sei $\sqrt{-15}$ eine fest gewählte Wurzel von -15 in $\mathbb{C}$. Zeigen Sie, dass $\mathbb{Z}[\sqrt{-15}]$ kein Hauptidealring ist.

Für diese sehr offen gestellte Aufgabe gibt es viele Wege nach Rom. Eine stellen wir hier ausführlich vor, eine weitere skizzieren wir (und greifen auf die erste Lösung zurück).
Lösung 1:
In der Vorlesung haben wir gesehen, dass in Hauptidealringen der Fundamentalsatz der Arithmetik in allgemeiner Form gilt. Jedes Element ist eindeutig als Produkt irreduzibler Elemente zu schreiben – eindeutig bis auf Reihenfolge und Multiplikation mit Einheiten.
Grundidee: Wir zeigen, dass $16 = 2\cdot 2\cdot 2\cdot 2$ und $16 = (1+\sqrt{-15})(1-\sqrt{-15})$ verschiedene Zerlegungen liefern. Dann sind wir fertig!

Die Elemente in $R := \mathbb{Z}[\sqrt{-15}]$ haben die Form $a + b\sqrt{-15}$ mit $a, b \in \mathbb{Z}$.
Für ein Element $a + b\sqrt{-15}$ definieren wir die *Norm* $N(a + b\sqrt{-15}) = a^2 + 15b^2$. Diese ist ganzzahlig.
Des Weiteren ist die Zuordnung $N\colon R \to \mathbb{Z}$, $r \mapsto N(r)$ multiplikativ, denn für alle $a, b, c, d \in \mathbb{Z}$ ist
$N((a + b\sqrt{-15})\cdot(c + d\sqrt{-15})) = N((ac + 15bd) + (ad + bc)\sqrt{-15}) = (ac - 15bd)^2 + 15(ad + bc)^2$
$= a^2c^2 - 30abcd + 125b^2d^2 + 15a^2d^2 + 30abcd + 15b^2c^2 = a^2c^2 + 125b^2c^2 + 25a^2d^2 + 15b^2c^2$
$= (a^2 + 15b^2)(c^2 + 15d^2) = N(a + b\sqrt{-15})N(c + d\sqrt{15})$.

Behauptung 1: Für $x \in R$ ist äquivalent:
(i) $x \in R^\times$.
(ii) $N(x) = 1$.
(iii) $x \in \{\pm 1\}$.
Beweis der Behauptung:
$(i) \to (ii)$: Wegen $N(1) = 1$ ist N ein Monoidhomomorphismus, bildet die Einheit x also auf eine Einheit in $\mathbb{Z}$, also 1 oder -1 ab. Aber wegen $N(x) \geq 0$ (das gilt sogar für alle x) folgt dann schon $N(x) = 1$.
$(ii) \to (iii)$: Der Ansatz $N(a + b\sqrt{-15}) = a^2 + 15b^2 \stackrel{!}{=} 1$ erzwingt $b = 0, a = \pm 1$.
$(iii) \to (i)$ ist klar.

Behauptung 2: 2 ist irreduzibel.
Ist $2 = xy$ eine Zerlegung, so ist $N(x)N(y) = N(2) = 4$. Da es aber kein Element mit Norm 2 gibt ($a^2 + 15b^2 = 2$ ist ganzzahlig nicht lösbar), folgt $\{N(x), N(y)\} = \{1, 4\}$, also ist x oder y eine Einheit.

Da alle Vielfachen von 2 von der Form $2(a + b\sqrt{-15}) = 2a + \ldots$ sind, sind $1 - \sqrt{-15}$ und $1 + \sqrt{-15}$ keine Vielfachen von 2.

Also ist $16 = 2\cdot 2\cdot 2\cdot 2$ eine Zerlegung in irreduzible Elemente und $16 = (1-\sqrt{-15})(1+\sqrt{-15})$ liefert eine andere. (Die beiden letzten Faktoren zerfallen gegebenenfalls weiter, aber der Faktor 2 kann nicht auftauchen.)

Lösung 2: Wir betrachten das von 2 und $1 + \sqrt{-15}$ erzeugte Ideal I von $R := \mathbb{Z}[\sqrt{-15}]$.
Zeige: Dies ist kein Hauptideal!
Zunächst gilt: Wäre I ein Hauptideal, so wäre der Erzeuger ein gemeinsamer Teiler von 2 und $1 + \sqrt{-15}$, aber – das berechnen wir genauso wie oben – diese Elemente sind teilerfremd, also wäre der Erzeuger eine Einheit, also $I = R$.
Des Weiteren rechnen wir nach, dass $\{2a + (1 + \sqrt{-15})b : a, b \in \mathbb{Z}\}$ ein Ideal ist (Abgeschlossenheit unter Multiplikation mit $\sqrt{-15}$?). Dieses Ideal ist dann I (denn I ist minimal unter allen Idealen, die 2 und $1 + \sqrt{-15}$ umfassen und jedes solche Ideal umfasst die obenstehende Menge) und an der Darstellung der Elemente sehen wir, dass $1 \notin I$ liegt. Das ist ein WIDERSPRUCH zu $I = R$.