Fragen im Zusammenhang mit der Zahlentheorie

12. Juli 2007

1 Fragen, die man sich stellen könnte ...

Im diesem ersten Teil sind einige Fragen zu den Begriffen und Definitionen der Vorlesung zusammengestellt. Das meiste ist recht prosaisch formuliert: Man sollte sich selbst überlegen, wie man die Fragen mathematisch exakt fassen kann bzw. welche Fassungen überhaupt sinnvoll sind.

Die Fragen sind nicht im Hinblick auf bestimmte Klausuraufgaben gestellt! Jegliche Zusammenhänge oder Ähnlichkeiten sind rein zufälliger Natur!
Es kann allerdings auch nicht schaden, sich zur Klausurvorbereitung Gedanken zu den hier angerissenen Themen zu machen.

Bitte bearbeitet diese Fragen jedoch erst, wenn ihr ALLE anderen Schritte zur Klausurvorbereitung abgeschlossen habt - oder gar nicht.

1. Euklidischer Algortihmus: Wie wird er in $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[X]$ angewendet?
   Was heißt *euklidisch* im Allgemeinen, also was ist ein *euklidischer* Ring?

2. Was ist ein Ideal?
   Gib eine Definition von *Ideal* an, die den Begriff des Moduls verwendet.
   Ist ein Ideal ein Unterring?

3. Was ist ein *Hauptidealring*, was ein *faktorieller* Ring?
   Setze die Begriffe *faktoriell*, *euklidisch* und *Hauptidealring* miteinander in Beziehung.

4. Wenn $\mathfrak{a}$, $\mathfrak{b}$ Ideale (in irgendeinem Ring) sind, ist dann auch $\{a \cdot b \mid a \in \mathfrak{a}, b \in \mathfrak{a}\}$ ein Ideal?
   Wenn nein: Gibt es Bedingungen unter denen $\{a \cdot b \mid a \in \mathfrak{a}, b \in \mathfrak{a}\}$ doch ein Ideal ist? Welche?

5. Was sind *prime* und was *irreduzible* Elemente in einem Ring?
   Was bedeutet es, wenn zwei Elemente eines Ringes *assoziiert* sind?

6. Was sind *Primideale* und was *maximale* Ideale eines Ringes?
   Wie stehen Primideale in Beziehung zu primen Elementen eines Ringes?
   Wie stehen maximale und Primideale miteinander in Beziehung (in Ganzheitsringen)?

7. Sei R ein Ring und $P \subset R$ ein Primideal.
   Zeige: $R \setminus P$ ist eine unter Multiplikation abgeschlossene Teilmenge von R.

8. Was ist ein *Körper-* und was ein *Ringhomomorphismus*?
   Worin unterscheiden sie sich?

9. Sei K ein Körper mit $\mathbb{Q} \subset K$ und $\phi : K \to K$ ein Körperhomomorphismus mit $\phi \mid_{\mathbb{Q}} = id_{\mathbb{Q}}$.
   Zeige: ϕ ist bijektiv.

10. Warum ist $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p ein Körper?
    Ist $\mathbb{Z}/p^2\mathbb{Z}$ ein Körper?
    Ist $\mathbb{Z}/6\mathbb{Z}$ ein Integritätsbereich?

11. Was gibt das *Legendre-Symbol* an?
    Was sind $\left(\frac{-1}{p}\right)$ und $\left(\frac{2}{p}\right)$?
    Wie steht $\left(\frac{-1}{p}\right)$ im Zusammenhang mit der Struktur von $\mathbb{F}_p$?

12. Was ist die *eulersche φ-Funktion*?
    Wie steht sie in Beziehung zur Struktur von $\mathbb{Z}/p^n\mathbb{Z}$ $(n \in \mathbb{N})$?
    Was ist $\varphi(m)$ für beliebiges $(m \in \mathbb{N})$?

13. Was ist eine Ganzheitsbasis in einem Erweiterungkörper von $\mathbb{Q}$?
    Gib jeweils eine Ganzheitsbasis des Ganzheitsringes von $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ quadratfrei, für die Fälle $d \equiv 1(4)$ und $d \not\equiv 1(4)$ an.
    Was sind jeweils die Minimalpolynome über $\mathbb{Q}$ der Elemente der Ganzheitsbasis?

14. Was besagt das Eisensteinkriterium?
    Gib ein Beispiel an, in dem man mit Hilfe des Eisensteinkriteriums zeigt, dass ein bestimmtes Polynom irreduzibel ist. (Man nennt ein solches Polynom dann auch *Eisensteinpolynom*).

15. Was sagt der Satz von Gauß über die Faktoren eines Produkts von Polynomen aus?
    In welchen Zusammenhang benutzt man diesen Satz (ständig)?

16. Chinesicher Restsatz: Wie wird er in $\mathbb{Z}$ angewendet?
    Wie lautet die abstrakte Fassung des Chinesischen Restsatzes, d.h. in allgemeinen Ringen?
    Formuliere den Chinesischen Restsatz in $\mathbb{Q}[X]$.

17. Was besagt der Elementarteilersatz?
    Formuliere diesen Satz sowohl für $\mathbb{Z}$-Moduln als auch für abelsche Gruppen.

2 Weiterführende Fragen und Probleme

Die hier formulierten Fragestellungen hängen zwar mit dem Vorlesungsstoff zusammen, gehen aber in Teilen auch darüber hinaus. Wer möchte, kann sich in den Semesterferien damit beschäftigen.
Wer im nächsten Semester *Algebra* oder später einmal *Algebraische Zahlentheorie* hören wird, wird diesen (oder ähnlichen) Problemen wiederbegegnen.

1. Sei $f \in \mathbb{Q}[X]$ und $\phi : \mathbb{Q} \to R$ ein Ringhomomorphismus. Sei $\Phi : \mathbb{Q}[X] \to R[Y]$ ein Ringhomomorphismus mit $\Phi \mid_{\mathbb{Q}} = \phi$ und $\Phi(X) = Y$.
   (Ist Φ wohldefiniert/eindeutig?)
   Zeige: Ist $\Phi(f)$ irreduzibel in $R[Y]$, so auch f in $\mathbb{Q}[X]$.
   Man muss eventuell fordern, dass f normiert ist; finde selbst heraus, ob dies o.ä. notwendig ist.

2. Bestimme alle irreduziblen Polynome vom Grad ≤ 4 in $\mathbb{Z}/3\mathbb{Z}[X]$.

3. Sei $f = \sum_{k=0}^{n} a_k X^k$ ein normiertes, irreduzibles Polynom vom Grad n aus $\mathbb{Q}[X]$ und sei x eine Nullstelle von f.
   Gib eine Basis von $\mathbb{Q}(x)$ als $\mathbb{Q}$-Vektorraum an.
   Für $n = 2$ handelt es sich einfach um eine quadratische Erweiterung, wie wir sie in der Vorlesung kennengelernt haben. Gib für diesen Fall Norm und Spur von x an und finde beide im Minimalpolynom von x wieder.
   Auch im allgemeinen Fall kann man die Folgende $\mathbb{Q}$-lineare Abbildung konstruieren:

$$\begin{aligned} M_x : \mathbb{Q}(x) &\to \mathbb{Q}(x) \\ z &\mapsto x \cdot z \end{aligned}$$

   Man definiert dann Norm und Spur von x wie folgt:

$$\begin{aligned} N(x) &:= \det(M_x) \\ Sp(x) &:= Spur(M_x) \end{aligned}$$

   Wie ist das Hauptpolynom von x definert? Unterscheidet es sich vom Minimalpolynom?
   Finde $N(x)$ und $Sp(x)$ im Minimalpolynom von x wieder.
   Sei nun $a \in \mathbb{Q}(x)$ beliebig (also i.A. $a \neq x$). Vollziehe obige Konstruktionen für a nach:
   Definiere und Berechne Norm, Spur, Haupt- und Minimalpolynom von a, indem du a in der oben gewählten Basis von $\mathbb{Q}(x)$ darstellst.
   Sind Norm, Spur, Haupt- und Minimalpolynom wohldefiniert?

4. Sei $(1, \omega)$ eine Ganzheitsbasis des Ganzheitsrings $\mathcal{O}_K$ einer quadratischen Erweiterung von $\mathbb{Q}$. $\{a, b\}$ habe die folgende Eigenschaft:

   $$\text{Für alle } \gamma \in \mathcal{O}_K \text{ existieren } z_1, z_2 \in \mathbb{Z} \text{ mit } \gamma = z_1 a + z_2 b.$$

   (Was unterscheidet $\{a, b\}$ von einer Ganzheitsbasis?)
   Dann gilt insbesondere:

   $$\begin{aligned} 1 &= z_{11} a + z_{12} b \\ \omega &= z_{21} a + z_{22} b \end{aligned}$$

   mit $z_{ij} \in \mathbb{Z}$.
   Setze $M := \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix}$ und bestimme $|\det M|$.

5. Sei K ein Körper und R sei gleichzeitig ein Integritätsbereich und ein endlich-dimensionaler Vektorraum über K. Zeige:
   R ist ein Körper.
   Warum ist ein Ganzheitsring dann kein Körper?

6. Zeige: In Ganzheitsringen, wie wir sie in der Vorlesung betrachtet haben, enthält jedes Primideal ein irreduzibles Element.

7. Zeige: Die einzigen Gruppen der Ordnung 4 sind $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Insbesondere sind alle Gruppen der Ordnung 4 abelsch.

8. Seien $n, m \in \mathbb{N}$. Zeige:
   $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ genau dann, wenn $(n, m) = 1$

3 Zum Abschluss

Am nächsten Freitag (20.07.07) findet noch eine Übung statt, in der z.B. die Klausur sowie offene Fragen besprochen werden können. Am 27.07.07 findet KEINE Übung mehr statt.

Viel Erfolg für die Klausur und
schöne Semesterferien.