Vorlesung zur Zahlentheorie (Osnabrück 2008)

Klausur

Dauer: Zwei volle Stunden + 10 Minuten Orientierung, in der noch nicht geschrieben werden darf. Hilfsmittel: Erlaubt ist lediglich ein DinA4-Blatt (zweiseitig) mit beliebigem Inhalt. Kein Taschenrechner etc. Alle Antworten sind zu begründen. Es gibt insgesamt 64 Punkte. Zum Bestehen braucht man 16 Punkte und für eine Eins braucht man 32 Punkte. Viel Glück!

Aufgabe 1. (4 Punkte)

Berechne mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Ergänzungssätze das Legendre-Symbol

$$\left(\frac{563}{1231}\right) .$$

Bemerkung: 563 und 1231 sind Primzahlen.

Aufgabe 2. (3 Punkte)

Wie viele Quadrate und wie viele primitive Elemente besitzt $\mathbb{Z}/(31)$?

Wie viele Elemente besitzt $\mathbb{Z}/(31)$, die weder primitiv noch ein Quadrat sind?

Sei x ein primitives Element von $\mathbb{Z}/(31)$. Liste explizit alle Elemente x^i auf, die weder primitiv noch ein Quadrat sind.

Aufgabe 3. (4 Punkte)

Sei $R = \mathbb{Z}[i]$. Berechne einen Erzeuger für das gebrochene Ideal aus $Q(R) = \mathbb{Q}[i]$, das durch die beiden Erzeuger

$$\frac{5}{7} \text{ und } \frac{-8+6i}{5}$$

gegeben ist.

Aufgabe 4. (6 Punkte)

Sei $R = \mathbb{Z}[\sqrt{-6}] \cong \mathbb{Z}[X]/(X^2+6)$. Berechne den Hauptdivisor zu

$$q = \frac{4}{5} + \frac{2}{3}\sqrt{-6} .$$

Aufgabe 5. (2 Punkte)

Man gebe zwei Primfaktoren von $2^{35} - 1$ an.

Aufgabe 6. (3 Punkte)

Bestimme ein Element aus $\mathbb{Z}[\sqrt{-11}]$, das unter allen Nichteinheiten minimale Norm besitzt. Begründe, dass dieses Element irreduzibel ist.

Aufgabe 7. (2 Punkte)

Man gebe ein Beispiel an, wo das Jacobi-Symbol den Wert 1 hat, aber kein Quadratrest vorliegt.

Aufgabe 8. (2 Punkte)

Betrachte die Quadratrestgruppe

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \ ,$$

wobei $\mathbb{Q}^{\times 2}$ die Untergruppe der Quadrate bezeichne. Zeige, dass es zu jeder Restklasse $x \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ einen Repräsentanten aus $\mathbb{Z}$ gibt.

Aufgabe 9. (4 Punkte)

Beschreibe mittels geeigneter Kongruenzbedingungen diejenigen ungeraden Primzahlen p mit der Eigenschaft, dass 7 ein Quadratrest modulo p ist.

Gibt es unendlich viele solche Primzahlen?

Aufgabe 10. (4 Punkte)

Sei p eine Primzahl und sei $f(x)$ ein Polynom mit Koeffizienten in $\mathbb{Z}/(p)$ vom Grad $d \geq p$. Zeige, dass es ein Polynom $g(x)$ mit einem Grad $< p$ gibt derart, dass für alle Elemente $a \in \mathbb{Z}/(p)$ die Gleichheit

$$f(a) = g(a)$$

gilt.

Aufgabe 11. (4 Punkte)

Finde die kleinste Zahl $n \geq 100$ derart, dass zugleich das reguläre n-Eck mit Zirkel und Lineal konstruierbar ist und dass n eine Summe von zwei Quadraten ist.

Aufgabe 12. (4 Punkte)

Beschreibe alle sechsten Einheitswurzeln im quadratischen Zahlbereich A_{-3} und im Restklassenring $\mathbb{Z}/(19)$ (eine n-te Einheitswurzel in einem Ring R ist ein Element x mit $x^n = 1$).

Aufgabe 13. (8 Punkte)

Sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und sei R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von null verschiedenes Ideal in R. Seien $b_1, \ldots, b_n \in \mathfrak{a}$ Elemente, die eine $\mathbb{Q}$-Basis von L bilden und für die der Betrag der Diskriminante

$$\triangle(b_1, \ldots, b_n)$$

unter all diesen Basen aus $\mathfrak{a}$ minimal sei.

Zeige, dass dann

$$\mathfrak{a} = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$$

ist. Man verwende hierzu elementare Eigenschaften der Diskriminante.

Aufgabe 14. (6 Punkte)

Sei $\mathbb{Z}_n$ die Nenneraufnahme zu n ($\mathbb{Z}_n$ besteht also aus allen rationalen Zahlen, die man mit einer Potenz von n als Nenner schreiben kann). Zeige, dass es nur endlich viele Unterringe R mit

$$\mathbb{Z} \subseteq R \subseteq \mathbb{Z}_n$$

gibt, und charakterisiere diese unter Verwendung der Primfaktorzerlegung von n.

Aufgabe 15. (4 Punkte)

Seien R und S Integritätsbereiche und sei $R \subseteq S$ eine ganze Ringerweiterung. Es sei $f \in R$ ein Element, das in S eine Einheit ist. Zeige, dass es dann schon in R eine Einheit ist.

Aufgabe 16. (4 Punkte)

Sei R ein Zahlbereich. Sei angenommen, dass R faktoriell ist. Zeige, dass dann R ein Hauptidealbereich ist. Dabei dürfen grundlegende Sätze über Zahlbereiche verwendet werden.