Heinrich Heine Universität Düsseldorf

PD Dr. Karin Halupczok
M.Sc. Thor Wittich

Zahlentheorie I (Algebraische Zahlentheorie), WiSe 22/23
Blatt 7

Aufgabe 1 (5 Punkte):
Sei R ein Ring und seien $(a_1, \dots, a_n)$ und $(b_1, \dots, b_m)$ zwei endlich erzeugte Ideale in R. Wir hatten nun schon oft benutzt, dass das Produkt dieser beiden Ideale durch

$$(a_1b_1, \dots, a_1b_m, \dots, a_nb_1, \dots, a_nb_m)$$

gegeben ist. Weisen Sie dies nach.

Aufgabe 2 (5 Punkte):
Sei p eine Primzahl und betrachten Sie das Ideal $(p) \subseteq \mathbb{Q}(\sqrt{2})$. Wir wollen die Primidealzerlegung von (p) mit Hilfe der expliziten Primidealzerlegung von Satz 12.15 bestimmen.

(i) Behandeln Sie den Fall $p = 2$ direkt.

(ii) Sei nun p ungerade. Nutzen Sie ein geeignetes Legendre-Symbol, um die Primfaktorzerlegung des Minimalpolynomes $\mu_{\sqrt{2}}$ in $\mathbb{F}_p[x]$ zu bestimmen.

(iii) Wie sieht nun die Primidealzerlegung von (p) aus?

Aufgabe 3 (5 Punkte):
In der Vorlesung haben wir die Verzweigungsindizes des Primideales $(2) \subseteq \mathbb{Z}$ in der Ringerweiterung $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ berechnet. In den nächsten beiden Aufgaben werden wir uns anschauen, wie die Situation bei den ungeraden Primzahlen aussieht. Sei p eine Primzahl mit $p = 3 \bmod 4$. Wir wollen zeigen, dass (p) auch aufgefasst als ideal in $\mathbb{Z}[i]$ immernoch prim ist.

(i) Nehmen Sie an, dass $p = \alpha\beta$ nicht prim ist. Zeigen Sie, dass $N(\alpha) = p = N(\beta)$ ist.

(ii) Begründen Sie kurz, dass die diophantische Gleichung $x^2 + y^2 = p$ keine Lösungen mod 4 besitzt und folgern Sie, dass obige Annahme falsch gewesen sein muss.

(iii) Geben Sie die Verzweigungsindizes von (p) in $\mathbb{Z}[i]$ an.

bitte wenden

Heinrich Heine Universität Düsseldorf

PD Dr. Karin Halupczok
M.Sc. Thor Wittich

Zahlentheorie I (Algebraische Zahlentheorie), WiSe 22/23
Blatt 7

Aufgabe 4 (5 Punkte):
Sei p eine Primzahl mit $p = 1 \bmod 4$.

(i) Nutzen Sie die Theorie der Legendre-Symbole, um zu zeigen, dass eine ganze Zahl m mit $p \mid m^2 + 1$ existiert.

(ii) Betrachten Sie die Inklusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ und begründen Sie mit Hilfe von (i), dass $p \in \mathbb{Z}[i]$ nicht prim ist.

(iii) Nutzen Sie die Norm von $\mathbb{Z}[i]$ um zu zeigen, dass in der Primfaktorzerlegung von $p \in \mathbb{Z}[i]$ genau zwei Faktoren (Multiplizität miteinbezogen) auftauchen.

(iv) Folgern Sie, dass sich p als $p = (a + ib)(a - ib)$ für zwei ganze Zahlen a und b schreiben lässt.

(v) Geben Sie die Verzweigungsindizes von (p) in $\mathbb{Z}[i]$ an.