

Universität des Saarlandes  
Fachrichtung 6.1, Mathematik  
Prof. Dr. Ernst-Ulrich Gekeler  
M.Sc. Philipp Stopp



**Probleme der Algebraischen Zahlentheorie,  
WS 2012/2013**

Die beiden folgenden Übungen sind Programmierübungen. Grundlage für beide Aufgaben ist das Programm PARI/GP, welches kostenlos auf der Seite

<http://pari.math.u-bordeaux.fr/>

erhältlich ist. Auf der Seite befindet sich auch eine ausführliche Dokumentation.

**Problem 5.**

Faktorisieren Sie

- (1)  $2^{2^7} + 1$  in  $\mathbb{Z}$ ,
- (2)  $X^{105} - 1$  über  $\mathbb{Q}$  und  $\mathbb{F}_7$ ,
- (3)  $X^{17} - 1$  über  $\mathbb{Q}(\sqrt{17})$ .

(Hierzu sind die folgenden Funktionen in PARI/GP hilfreich: `Mod`, `factor`, `factornf`)

**Problem 6.**

- (1) Benutzen Sie PARI/GP um für den Körper  $K = \mathbb{Q}(\sqrt{-21})$  die Klassen-  
gruppe und deren Struktur zu bestimmen. Geben Sie Repräsentanten der  
einzelnen Idealklassen an. Verifizieren Sie mit Hilfe von PARI/GP, dass  
 $I_1 = 4\mathbb{Z} + (2 + 2\sqrt{-21})\mathbb{Z}$  und  $I_2 = 10\mathbb{Z} + (4 + 2\sqrt{-21})\mathbb{Z}$  ganze Ideale von  $K$   
sind und bestimmen Sie deren Norm und  $\mathbb{Z}$ -Basen für  $(I_1)^{-1}$ ,  $I_1 \cap I_2$ ,  $I_1 +$   
 $I_2$ ,  $I_1 * I_2$  und  $I_1/I_2$ . Zerlegen Sie  $I_1, I_2$  in Primideale.  
(Hinweis: In der Dokumentation von PARI/GP finden Sie die Funktionen  
`bnfinit`, `nfisideal`, `idealnrm`, `idealinv`, `idealadd`, `idealmul`,  
`idealfactor`, etc.. Insbesondere ist die Klassengruppe von  $L = \text{bnfinit}(f(x))$   
durch `L.clgp` gegeben.)
- (2) Zählen Sie ab wieviele ganze Ideale jeder Idealklasse von  $K$  aus (1) eine  
Norm kleiner als 10000 haben. Gibt es gravierende Unterschiede von Klasse  
zu Klasse oder herrscht in etwa Gleichverteilung?  
(Hinweis: Hilfreich sind hier insbesondere `ideallist`, `bnfisprincipal`.)
- (3) Durchlaufen Sie alle imaginärquadratischen Zahlkörper deren Diskriminan-  
ten höchstens den Absolutbetrag 5000 haben und zählen Sie für  $r = 1, 2, 3, 4$   
wieviele der Körper eine Klassengruppe vom Rang  $r$  haben. Was fällt auf?