**Algorithmic Number Theory**
WS 19/20

Prof. Dr. Ulrich Thiel
University of Kaiserslautern

# Exercise Sheet 11

Jan 20, 2020

For the first two exercises you can find detailed solutions in the excellent write-ups by Keith Conrad, available at https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf and https://kconrad.math.uconn.edu/blurbs/gradnumthy/classgpex.pdf. Please first try to do them yourself, it's fun.

***Exercise 1.*** Compute the ideal factorization of the following prime numbers $p$ in the following number fields:

(a) $p = 2, \ldots, 13$ in $\mathbb{Q}(\sqrt{10})$
(b) $p = 2, \ldots, 13$ in $\mathbb{Q}(\sqrt{5})$
(c) $p = 3, 5, 7, 11, 73$ in $\mathbb{Q}(\sqrt[4]{2})$
(d) $p = 3, 5$ in $\mathbb{Q}(\alpha)$, where $\alpha$ is a root of $X^3 + 2X + 22$
(e) $p = 3, 7$ in $\mathbb{Q}(\sqrt[3]{10})$
(f) $p = 3, 503$ in $\mathbb{Q}(\alpha)$, where $\alpha$ is a root of $X^3 - X^2 - 2X - 8$. Why is $p = 2$ difficult?[1]

***Exercise 2.*** Compute the class group of the ring of integers of the following number fields:

(a) $\mathbb{Q}(\sqrt{82})$
(b) $\mathbb{Q}(\sqrt{-14})$
(c) $\mathbb{Q}(\sqrt{-30})$
(d) $\mathbb{Q}(\sqrt{79})$
(e) $\mathbb{Q}(\sqrt{-65})$

***Exercise 3.*** Give a simple and direct proof of the fundamental equation for the splitting of prime ideals in the ring of integers of number fields by using the finiteness of the class number in this case.[2]

---

[1] The answer to this question also gives a counter-example to the claim in Exercise I.8.2 in J. Neukirch's book.

[2] The ideal norm and its multiplicativity will be helpful as well.