Algorithmic Number Theory
WS 19/20

Prof. Dr. Ulrich Thiel
University of Kaiserslautern

Exercise Sheet 10

Jan 13, 2020

Exercise 1. Let R be a Dedekind domain. Let I, J be fractional ideals of R.

(a) We say that I *divides* J, denoted $I|J$, if there is an ideal $C \subseteq R$ such that $IC = J$. Show that $I|J$ if and only if $J \subseteq I$.

(b) Show that $\gcd(I, J) = I + J$ is the greatest common divisor of I and I.

Remark. Exercise 1a implies: if R is the ring of integers in a number field, then the prime ideals occurring in the factorization of the ideal pR for a prime number $p \in \mathbb{Z}$ are precisely the prime ideals lying over p.

Exercise 2. Let R be a Dedekind domain and let $I \subseteq R$ be a non-zero ideal. Show that for any $0 \neq a \in I$ there is $b \in R$ such that $I = (a, b)$. In particular, any ideal of R is generated by at most 2 elements.[1]

Exercise 3. Determine the class group of the following number fields:

(a) $\mathbb{Q}(\sqrt{-5})$

(b) $\mathbb{Q}(\sqrt{d})$ for $d = -3, -2, -1, 2, 3, 5, 13$

(c) $\mathbb{Q}(\zeta_5)$

Exercise 4. Let $K \subset L$ be a finite extension of number fields. For an $\mathcal{O}_K$-submodule M of L define

$$M_K^* := \{\alpha \in L \mid \mathrm{Tr}_{L|K}(\alpha M) \subseteq \mathcal{O}_K\} .$$

Show that if I is a fractional ideal of $\mathcal{O}_L$, then so is I_K^*. (Hint: trace form).

[1] Note that $(a, b) = \gcd((a), (b))$, so you need to show that I is the greatest common divisor of (a) and (b). Use prime factorization of ideals, and use the Chinese Remainder Theorem to find b.