ALGEBRAIC NUMBER THEORY

REVIEW

Of course you need to be familiar with the basic definitions: quadratic number fields, norm, trace, integral elements, integral basis, discriminant, $\mathbb{Z}$-modules, $\mathcal{O}_K$-modules, orders, ideals (prime, irreducible, maximal), norms of modules and ideals, units, Pell equation.

Among the basic results I would count:

- The algebraic integers inside some quadratic number field K form a ring.
- Full modules have finite norm. If M is a full module, then $MM' = N(M)\mathcal{O}$ for some order $\mathcal{O}$.
- If $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$, then $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$.
- In $\mathcal{O}_K$, an ideal is prime iff it is irreducible iff it is maximal.
- In $\mathcal{O}_K$, $\mathfrak{a} \subseteq \mathfrak{b}$ iff $\mathfrak{b} \mid \mathfrak{a}$.
- $\mathcal{O}_K$ is a Dedekind ring, i.e., every nonzero ideal is a product of prime ideals, and this factorization is unique up to order.
- The Pell equation $x^2 - my^2 = 1$ has a nontrivial solution for every squarefree natural number m.
- The unit group of $\mathcal{O}_K$ satisfies $\mathcal{O}_K^\times \simeq W \oplus \mathbb{Z}^r$, where W is a finite group (the group of roots of unity inside K) and where $r = 0, 1$ according as K is complex or real.
- The decomposition law in quadratic extensions.

You should be able to

- reduce algebraic integers modulo a given ideal, i.e. compute $\alpha \bmod \mathfrak{a}$ (or at least check whether two given elements are congruent modulo $\mathfrak{a}$).
- test whether a given ideal is principal (using units if K is real; you need not memorize the best possible bounds – the idea is important).
- find the prime ideal factorization of a given element α.
- compute the fundamental unit by solving the Pell equation by trial and error (if it is small) or by constructing elements of equal norm.