Appendix: Dirichlet's unit theorem

Definition: Let K be an algebraic number field. Let
$\mu_K := \{\alpha \in K \mid \alpha \text{ is a root of unity}\} = \{\alpha \in K \mid \exists n \in \mathbb{N} : \alpha^n = 1\}$.

Lemma Let K be an algebraic number field. Then $(\mu_K, \cdot)$ is a subgroup of $(\mathcal{O}_K^*, \cdot)$.

Proof: $\alpha \in \mu_K \Rightarrow \exists n \in \mathbb{N} : \alpha^n = 1$. Then $\alpha \in \mathcal{O}_K$ as α is a root of $X^n - 1 \in \mathbb{Z}[X]$ and $\alpha \in \mathcal{O}_K^*$ as $\alpha \cdot \alpha^{n-1} = 1$. If $\alpha, \beta \in \mu_K \Rightarrow \exists n, m \in \mathbb{N} : \alpha^n = \beta^m = 1 \Rightarrow (\alpha\beta^{-1})^{mn} = 1$, i.e., $\alpha\beta^{-1} \in \mu_K$.

Theorem (Dirichlet's unit theorem [dt. Dirichletscher Einheitensatz]) Let K be an algebraic number field.

(i) $(\mathcal{O}_K^*, \cdot)$ is a finitely generated abelian group,

(ii) $\mathcal{O}_K^*$ is the direct product of μ_K and a free abelian group of rank $r+s-1$,

(iii) μ_K is a finite cyclic group of even order.

Remark: That μ_K is a finite group implies that is a cyclic group (as $(\mu_K, \cdot)$ is a finite subgroup of $(K^*, \cdot)$). The order of μ_K has to be even by Lagrange's theorem as it contains the subgroup $\{1, -1\}$.

Corollary Let K be an algebraic number field. Then the following are equivalent:

(i) $\mathcal{O}_K^*$ is finite,

(ii) $K = \mathbb{Q}$ or K is an imaginary quadratic field.

Proof: $\mathcal{O}_K^*$ is finite $\Leftrightarrow r+s-1 = 0 \Leftrightarrow r+s = 1 \Leftrightarrow (r,s) \in \{(1,0), (0,1)\}$
$\Leftrightarrow K = \mathbb{Q}$ (if $(r,s) = (1,0)$) or K is imaginary quadratic (if $(r,s) = (0,1)$)

Corollary Let K be a real quadratic number field. There is a $\eta \in \mathcal{O}_K^*$, $\eta > 1$ such that $\mathcal{O}_K^* = \{\pm \eta^n \mid n \in \mathbb{Z}\}$.

Proof: As $K \subseteq \mathbb{R}$ we see $\mu_K = \{1, -1\}$ and $r+s-1 = 2+0-1 = 1$. Dirichlet's unit theorem implies that $\exists \lambda \in \mathcal{O}_K^* : \mathcal{O}_K^* = \{\pm \lambda^n \mid n \in \mathbb{Z}\}$. Clearly $-\lambda, \lambda^{-1}$ and $-\lambda^{-1}$ have the same property, but only one of them is >1, i.e., choose $\eta \in \{\lambda, -\lambda, \lambda^{-1}, -\lambda^{-1}\}$ with $\eta > 1$.

Remarks: 1) The $\eta \in \mathcal{O}_K^*, \eta > 1$ such that $\mathcal{O}_K^* = \{\pm \eta^n \mid n \in \mathbb{Z}\}$ is called fundamental unit.

2) We determined the fundamental unit for $K = \mathbb{Q}(\sqrt{2})$ (where $\eta = 1+\sqrt{2}$) in Theorem 73 and for $K = \mathbb{Q}(\sqrt{3})$ (where $\eta = 2+\sqrt{3}$) in Exercise 33.

3) There is no simple formula for the fundamental unit but algorithms.

4) More generally $r+s-1 = 1 \Leftrightarrow r+s = 2 \Leftrightarrow (r,s) \in \{(2,0), (1,1), (0,2)\}$
$\Leftrightarrow K$ is real quadratic (if $(r,s) = (2,0)$) or
or K is cubic with exactly one real embedding (if $(r,s) = (1,1)$)
or K is totally imaginary quartic (if $(r,s) = (0,2)$).