Exercise 1. Prove the norm and trace formulas from lecture, that for $L/K$ separable, $N_{L/K}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$, and $\text{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$, in the following steps:

(1) Show that if $\alpha \in L$, and $f(x) \in K(x)$ is the monic minimal polynomial for $\alpha$, with degree $d$, then $\det(xI - m_\alpha) = f(x)^{n/d}$.

(2) Using the fact that if $E/F$ is a separable field extension of finite degree, then any imbedding $E \rightarrow \bar{F}$ has exactly $[F:E]$ extensions to imbeddings $F \rightarrow \bar{F}$, show that in the above notation, $f(x)^{n/d} = \prod_{i=1}^n (x - \sigma_i(\alpha))$.

(3) Conclude the statements on the norm and trace by comparing with the appropriate coefficients of $\det(xI - m_\alpha)$.

Exercise 2. Using integrality of the norm and trace, check that for $n \in \mathbb{N}$ square-free, the ring of integers of $\mathbb{Q}(\sqrt{n})$ is given as $\{a + b\omega : a, b \in \mathbb{Z}\}$, and where $\omega$ is given as follows:

(I) if $n \not\equiv 1 \pmod{4}$, then $\omega = \sqrt{n}$;

(II) if $n \equiv 1 \pmod{4}$, then $\omega = \frac{1 + \sqrt{-n}}{2}$.

Exercise 3. Show that an element $\alpha$ of a ring of integers $\mathcal{O}_K$ is a unit if and only if its norm over $\mathbb{Q}$ is $\pm 1$. Show that in the case that $K$ is Galois over $\mathbb{Q}$, this still holds for any ring $R \subset \mathcal{O}_K$ which is Galois invariant.

Conclude that in particular, $x + y\sqrt{-n}$ is a unit in $\mathbb{Z}[\sqrt{n}]$ if and only if $x, y$ is a solution to either the Pell equation $x^2 - ny^2 = 1$ or the equation $x^2 - ny^2 = -1$ (observe, however, that if $x+y\sqrt{-ny}$ is a solution to $x^2 - ny^2 = -1$, then $(x+y\sqrt{-ny})^2$ is a solution to the Pell equation).

Let $p \in \mathbb{Z}$ be a prime number, and suppose that $p = \alpha\beta$ for some non-units $\alpha, \beta \in \mathbb{Z}[\sqrt{-n}]$. Show that $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.

Recall that an integral domain $R$ is said to be a Euclidean domain if there exists a norm map $N : R \rightarrow \mathbb{N} \cup \{0\}$ satisfying:

(i) $N(r) = 0$ if and only if $r = 0$;

(ii) For all $a, b \in R$, with $b$ non-zero, there exist $q, r \in R$ such that $a = bq + r$, and $N(r) < N(b)$.

Recall that a Euclidean domain is a principal ideal domain, hence a unique factorization domain.

Exercise 4. Show that $\mathbb{Z}[\sqrt{n}]$ is a Euclidean domain if $n = -2, -1, 2$ or 3.

Exercise 5. Fix an $n \in \mathbb{N}$. Observe that if $m = p_1^{e_1} \cdots p_k^{e_k}$, and for each $i$, either $e_i$ is even, or $p_i$ can be written in the form $x^2 + ny^2$, then $m$ can be written in this form. Show that the converse is also true if $n = 1$ or 2.

On the other hand, show by counterexample that the converse is false if $n = 5$. 

BRIAN OSSERMAN