Reminder: An algebraic number field F is a field containing $\mathbb{Q}$ such that every $\alpha \in F$ is algebraic over $\mathbb{Q}$ and F has finite dimension n (called the degree) as a vector space over $\mathbb{Q}$. An $\alpha \in F$ is an algebraic integer if it is the root of a monic polynomial with integer coefficients. The set $D = \{\alpha \in F : \alpha \text{ is an algebraic integer } \}$ is a Dedekind domain called the ring of integers of F.

Theorem 30.1. Let F be an algebraic number field of degree n. Then there are n distinct field embeddings (i.e., injective homomorphisms) $\sigma_i : F \to \mathbb{C}$. Each σ_i is the identity map on $\mathbb{Q}$.

Alternative definition of norm: For $\alpha \in F$ we have $N_F(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.

Reminder: An ideal $I \subseteq D$ is a subgroup under $+$ such that $ID \subseteq I$. The product of two ideals I_1 and I_2 of D is $I_1 I_2 = \{\sum_{i=1}^{n} \alpha_i \beta_i : n \in \mathbb{N}, \alpha_i \in I_1, \beta_i \in I_2\}$. A principal ideal, denoted (α), is $\{\alpha\beta : \beta \in D\}$ for some $\alpha \in D, \alpha \neq 0$.

Exercise 30.2. Prove that a principal ideal is an ideal. Prove that the product of two ideals is an ideal. Prove that $(\alpha_1)(\alpha_2) = (\alpha_1\alpha_2)$.

Definition 30.3. A *fractional ideal* is a subset $I \subseteq F$ such that

(1) I is a subgroup of F under $+$
(2) $ID \subseteq I$
(3) there is some $\beta \in D, \beta \neq 0$ such that $(\beta)I \subseteq D$.

Exercise 30.4. Prove than an ideal is a fractional ideal. Prove that if I is a fractional ideal and if $(\beta)I \subseteq D$ then $(\beta)I$ is an ideal. For any $\alpha \in F^*$ define $(\alpha) = \{\alpha\beta : \beta \in D\}$. Prove that (α) is a fractional ideal (called a principal fractional ideal).

Lemma 30.5. Let I be an ideal, then the set $I^{-1} = \{\alpha \in F : \alpha I \subseteq D\}$ (introduced in Lecture 16) is a fractional ideal.

Definition 30.6. Two fractional ideals I_1 and I_2 are *equivalent* if there exist $\alpha, \beta \in D$ such that $(\alpha)I_1 = (\beta)I_2$. We write $I_1 \sim I_2$ if I_1 and I_2 are equivalent. Write $[I]$ for the set of all fractional ideals equivalent to I.

Exercise 30.7. Prove that $\sim$ is an equivalence relation. Prove that $I \sim D$ if and only if I is a principal fractional ideal.

Definition 30.8. $C_F = \{[I] : I \text{ is a fractional ideal of } F\}$.

Theorem 30.9. C_F is a group.

Alternative interpretation: C_F is in one-to-one correspondence with the quotient group of all non-zero fractional ideals modulo the set of all principal fractional ideals $(\alpha) = \{\alpha\beta : \beta \in D\}$ for $\alpha \in F^*$.

A major theorem in algebraic number theory is that the ideal class group is a finite group. We now prove this, first giving two necessary lemmas.

Lemma 30.10. Let F be an algebraic number field. There exists $m_F \in \mathbb{N}$ such that, for all $\gamma \in F$ there exist $t \in \mathbb{N}$ with $1 \leq t \leq m_F$ and $\omega \in D$ satisfying $|N_F(t\gamma - \omega)| < 1$.

Proof. Let n be the degree of F and let $\omega_1, \ldots, \omega_n$ be a basis for D as a $\mathbb{Z}$-module.
Let $\gamma = \sum c_i \omega_i$ with $c_i \in \mathbb{Q}$. Using the complex embeddings σ_j to compute the norm, we obtain

$$|N_F(\gamma)| = \left| \prod_j \left(\sum_i c_i \sigma_j(\omega_i) \right) \right| \leq C(\max_i |c_i|)^n \tag{1}$$

where $C = \prod_j (\sum_i |\sigma_j(\omega_i)|)$. Choose $m \in \mathbb{N}$ such that $m^n > C$ and set $m_F = m^n$.
Denote $a_i = \lfloor c_i \rfloor \in \mathbb{Z}$ so that $c_i = a_i + b_i$ where $0 \leq b_i < 1$. Define $[\gamma] = \sum_i a_i \omega_i \in D$ and $\{\gamma\} = \sum_i b_i \omega_i$. Then, $\gamma = [\gamma] + \{\gamma\}$.
Define $\phi : F \to \mathbb{Q}^n$ by $\phi(\sum_i c_i \omega_i) = (c_1, \ldots, c_n)$. Then $\phi(\{\gamma\})$ lies in the unit cube $[0,1)^n$. Partition the unit cube into m^n subcubes of side length $1/m$. Consider the points $\phi(\{k\gamma\})$ for $1 \leq k \leq m^n + 1$. By the pigeonhole principle at least two of them, say, $\{r\gamma\}$ and $\{s\gamma\}$ with $1 \leq r < s \leq m^n + 1$, lie in the same subcube. Set $t = s - r$ so that $t\gamma = \omega + \delta$ where $\omega \in D$ and the coordinates of δ have absolute values $\leq 1/m$. It follows from equation (1) that $|N_F(\delta)| \leq C(1/m)^n < 1$. □

Lemma 30.11. Let k be an integer. There are only finitely many ideals $I \subseteq D$ such that $k \in I$.

Proof. There is a homomorphism of additive groups $\phi : D \to (\mathbb{Z}/k\mathbb{Z})^n$ with kernel (k), namely $\phi(\sum_i c_i \omega_i) = (c_1 \mod k, \ldots, c_n \mod k)$. Since $(k) \subseteq I \subseteq D$ it follows that $\phi(I)$ is a subgroup of $(\mathbb{Z}/k\mathbb{Z})^n$. Conversely, any subgroup of $(\mathbb{Z}/k\mathbb{Z})^n$ corresponds to a unique additive subgroup I of D such that $(k) \subseteq I$. Since there are only finitely many subgroups of $(\mathbb{Z}/k\mathbb{Z})^n$ the result follows. □

Theorem 30.12. The ideal class group of an algebraic number field is finite.

Proof. Let $J \subset D$ be an ideal and let $0 \neq \alpha \in J$; then $0 \neq N_F(\alpha) \in \mathbb{Z}$. Choose $0 \neq \beta \in J$ with $|N_F(\beta)|$ minimal. By Lemma 30.10, for any $\alpha \in J$ we have $|N_F(t\alpha - \omega\beta)| < |N_F(\beta)|$ for some $\omega \in D$ and $1 \leq t \leq m_F$. Since $t\alpha - \omega\beta \in J$ it follows that $t\alpha = \omega\beta$, and so $t\alpha \in (\beta)$. Hence $(m_F!)J \subset (\beta)$. Let $I = (1/\beta)(m_F!)J \subset D$; then, I is an ideal and $(m_F!)J = (\beta)I$, that is, $J \sim I$. Since $\beta \in J$, we have $m_F!\beta \in (\beta)I$ and hence $m_F! \in I$.
In other words, we have shown that every ideal J is equivalent to an ideal I such that $m_F! \in I$. The result now follows from Lemma 30.11, since there can only be finitely many ideals containing $m_F!$. □

Definition 30.13. The order of the ideal class group C_F is called the *class number* and is denoted h_F.