Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Lectures 4-5: Ideals and Unique Factorization
September 5 and 7, 2001

Reference. Neukirch, Section 1.3.

Jargon watch. A *Dedekind domain* is an integral domain R such that:

- R is noetherian (every ideal in R is finitely generated);
- R is integrally closed (in its field of fractions);
- every nonzero prime ideal of R is maximal.

Examples: $\mathbb{Z}$ and $K[x]$ for any field K. Nonexample: $K[x, y]$, because the ideal (x) is prime but not maximal.

Outline of lectures.

1. Define ideal, prime ideal, principal ideal, multiplication of ideals, divisibility of ideals.
2. Define Dedekind domain. Show that the ring of integers in a number field is a Dedekind domain. Point out that proper subrings of the ring of integers need not be Dedekind domains.
3. State the unique factorization theorem: every nonzero ideal in a Dedekind domain can be uniquely written as a product of prime ideals.
4. Define fractional ideals, inverse of an ideal. Show that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$ for $\mathfrak{p}$ prime. For ideals in a ring of integers, reformulate in terms of the absolute norm.
5. Prove existence, uniqueness of prime factorizations.
6. Formulate, prove Chinese Remainder Theorem for ideals.
7. Define ideal group, ideal class group. Mention that the ideal class group of a number field is finite (to be proved later).

Addenda to Friday's lecture (August 31). I was asked at the end of class why the discriminant is an invariant of the basis. If $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_n$ are two bases of K spanning the same $\mathbb{Z}$-submodule, then there is an invertible matrix M with entries in $\mathbb{Z}$ such that $\alpha_i = \sum_j M_{ij}\beta_j$. Then

$$\begin{aligned}
\operatorname{disc}(\alpha_1, \dots, \alpha_n) &= \det(\sigma_i(\alpha_j))^2 \\
&= \det(M)^2 \sigma_i(\beta_j)^2 \\
&= \det(M)^2 \operatorname{disc}(\beta_1, \dots, \beta_n).
\end{aligned}$$

Since M is invertible with entries in $\mathbb{Z}$, its determinant is ± 1, and $\det(M)^2$ must be 1. So the discriminants are the same.

I was also asked how to prove that $\mathfrak{o}_K$ is free of rank n (where $n = [K : \mathbb{Q}]$). The answer I gave in class was that from the properties of the discriminant, it follows that $\mathfrak{o}_K$ contains a subgroup of finite index which is free of rank n. (The square of that index must divide the discriminant.) Alternatively, the $\mathbb{Z}$-module of elements of $\mathfrak{o}_K$ with integral trace is free of rank n, and the ring of integers is a submodule thereof with finite index.