Lecture 2-24: Discriminants and integers in cyclotomic fields; general Dedekind domains

February 24, 2025

I now introduce a tool that is useful in useful for studying both rings of integers and Galois groups of polynomials. I will use this to prove that the obvious formula for $R_n = \mathcal{O}_{K_n}$ is in fact the correct one, where $K_n = \mathbb{Q}[\epsilon_n] = \mathbb{Q}[e^{2\pi i/n}]$, if n is prime (it actually holds in general).

Definition 3.1, p. 6

Given the ring of integers $R = \mathbb{O}_K$ in a number field K of degree n over $\mathbb{Q}$ and elements $\alpha_1, \ldots, \alpha_n$ of K, the *discriminant* $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ of the α_i is the square of the determinant of the $n \times n$ matrix M whose *ij*th entry is $\sigma_i(\alpha_j)$, where $\sigma_1, \ldots, \sigma_n$ are the distinct embeddings of the field K into $\mathbb{C}$.

This quantity is 0 if the α_i are dependent over $\mathbb{Q}$, since then the matrix M has dependent columns. Otherwise it makes sense as an element of $\mathbb{Q}^*$, since it is fixed by the Galois group G of the Galois closure $\bar{K}$ of K in $\mathbb{C}$. It is nonzero because the embeddings σ_i are independent over $\bar{K}$, by the same argument that automorphisms in G are independent as functions on $\bar{K}$. It is independent of the ordering of the α_i or σ_j, since changing either or both of these orderings changes the determinant by a sign at most, which disappears on taking the square.

If the α_i form a $\mathbb{Z}$-basis of R, then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ is called the discriminant of R and denoted $\operatorname{disc}(R)$. This makes sense since any other $\mathbb{Z}$-basis $\{\beta_i\}$ of R has $(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n)A$ for some $A \in GL_n(\mathbb{Z})$, which must have determinant ± 1. Finally, it always lies in $\mathbb{Z}$ if the α_i lie in R, since then it is an algebraic integer fixed by G and so is rational. More generally, we define $\operatorname{disc}(S)$ for any $\mathbb{Z}$-submodule S of R of rank n as $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ for any $\mathbb{Z}$-basis (α_i) of S; as with R this definition is independent of the choice of basis.

Lemma 3.16, p. 9

With notation as above, we have $\operatorname{disc}(S) = \operatorname{disc}(R) N(S)^2$.

Proof.

Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be $\mathbb{Z}$-bases of R and S, respectively, with $(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n)A$ for some $A \in M_n(\mathbb{Z})$. The definition of discriminant shows that $\mathrm{disc}(S) = \mathrm{disc}(R) \det^2 B$ and it is not difficult to check that $N(S) = |\det B|$, so I am done. $\square$

As an immediate corollary, I get that the norm of a principal ideal (α) of R is the absolute value of the norm $N(\alpha)$ of α, since then if $\alpha_1, \ldots, \alpha_n$ is a basis of R, then $\alpha\alpha_1, \ldots, \alpha\alpha_n$ is a basis of (α) and the discriminant of the second basis is $N(\alpha)^2$ times the discriminant of the first one.

An especially convenient basis to use in computing disc(R) or disc(S) arises as follows. By the Primitive Element Theorem, we have $K = \mathbb{Q}[\alpha]$ for some α. Then $D = \mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) \neq 0$ since the powers α_i are independent over $\mathbb{Q}$. Writing the Galois conjugates of α as $\alpha_1 = \alpha, \ldots, \alpha_n$, we see that the ijth entry of the matrix M in the definition of D is α_i^{j-1}, whence M is a so-called Vandermonde matrix. Its determinant is well known to be $\prod_{i>j}(\alpha_i - \alpha_j)$, since when regarded as a function of the variables α_i, it vanishes whenever two of these variables are equal and the coefficient of $\alpha_n^{n-1}\alpha_{n-1}^{n-2}\ldots\alpha_2$ in it is 1.

Letting f be the minimal polynomial of the α_i over $\mathbb{Q}$, we see that *D is the product of the squared differences of the roots of f*. This product of squared differences of the roots of a polynomial is called the discriminant of the polynomial. It is 0 if and only if the polynomial has two equal roots and is fixed by the Galois group of the polynomial.

Computing the discriminant of $\mathcal{O}_K$ for a quadratic extension $K = \mathbb{Q}[\sqrt{d}]$ with d a square-free integer, we get $(2\sqrt{d})^2 = 4d$ if $d \not\equiv 1 \bmod 4$ and $(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2})^2 = d$ if $d \equiv 1 \bmod 4$. Here I am using the basis $(1, \sqrt{d})$ in the first case and $(1, \frac{1+\sqrt{d}}{2})$ in the second one. The other specific field mentioned last time, namely the cyclotomic field K_p corresponding to the prime $p > 2$, is harder to compute, since I have not yet given a basis for its ring of integers R_p. I first calculate the discriminant of a particular set of elements in R_p and then show that this coincides with the discriminant of R_p itself.

For this purpose I need a general result.

Proposition 3.10, p. 8

Let $K = \mathbb{Q}[\alpha]$ be a number field of degree n, f the minimal polynomial of α over $\mathbb{Q}$. Then $D = \mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\binom{n}{2}} N(f'(\alpha))$, where $N(f'(\alpha))$ denotes the norm of $f'(\alpha)$.

I showed above that $\prod_{i<j}(\alpha_i - \alpha_j)^2$, where $\alpha_= \alpha, \ldots, \alpha_n$ are the Galois conjugates of α, so that $f = \prod_{i=1}^{n}(x - \alpha_i)$. Evaluating $f'(\alpha)$ and $N(f'(\alpha))$ by the product rule, the result follows at once.

I need a couple of other calculations. Let $\epsilon = e^{2\pi i/p}$ be s primitive pth root of 1 in $\mathbb{C}$. Recall that the minimal polynomial of ϵ over $\mathbb{Q}$ is the pth cyclotomic polynomial $\Phi_p = \frac{x^p-1}{x-1} = 1 + \cdots + x^{p-1}$.

Lemma 8.3, p. 27

We have $N(1-\epsilon^i) = p$ for $1 \leq i \leq p-1$. The differences $1-\epsilon^i$ are unit multiples of each other. We have
$\mathrm{disc}(1, \epsilon, \ldots, \epsilon^{p-2}) = (-1)^{\binom{p}{2}} p^{p-2} = (-1)^{\frac{p-1}{2}} p^{p-2}$.

Proof.

The conjugates of ϵ are the powers ϵ^i. Then we have $N(1-\epsilon) = (1-\epsilon)\cdots(1-\epsilon^{p-1}) = g'(1) = p$, by the product rule, where $g = x^p - 1$. The other differences $1-\epsilon^i$ are conjugates of $1-\epsilon$, so have the same norm. Given any two differences $1-\epsilon^i, 1-\epsilon^j$, there are integers a, b with $ia = j, jb = i \bmod p$, whence $1-\epsilon^i, 1-\epsilon^j$ are multiples and thus unit multiples of each other. To compute the discriminant, apply Proposition 3.10 above; here $\alpha = \epsilon, f = \Phi_p, f'(\alpha) = p\frac{\epsilon^{p-1}}{\epsilon-1}$, by the quotient rule. $\square$

Now I can finally state the main result. Set $S = \mathbb{Z}[\epsilon]$.

Proposition 8.4, p. 28

With notation as above, we have $R_p = S = \mathbb{Z}[\epsilon]$.

Proof.

Lemma 8.3 shows that $\mathrm{disc}(S) = (-1)^{\frac{p-1}{2}} p^{p-2}$. By Lemma 3.16, the finite group R_p/S has order a power of p, whence there is N with $p^N R_p \subset S$. Since $N(1-\epsilon) = p$, the finite group $R_p/(1-\epsilon)$ has order p, whence its elements are the cosets of $0, \ldots, p-1$. Given $z \in R_p$ we can write $z = a_0 + (1-\epsilon)z_1$ for some $a_0 \in \mathbb{Z}, z_1 \in R_p$ and then $z = a_0 + (1-\epsilon)a_1 + (1-\epsilon^2)z_2$ for some $a_1 \in \mathbb{Z}, z_2 \in R_p$. Continuing in this way, we write $z + a_0 + (1-\epsilon)a_1 + (1-\epsilon)^2 a_2 + \ldots + (1-\epsilon)^{(p-1)N} z_{(p-1)N}$ for some $a_i \in \mathbb{Z}, z_{(p-1)N} \in R_p$. But now the power $(1-\epsilon)^{p-1}$ is a unit multiple of p and $p^N R_p \subset S$, whence finally $z \in S$, as desired. $\square$

The proof shows that the prime p is ramified in R_p; that is (as defined last time) the ideal p is the $(p-1)$st power of an ideal in R_p. It turns out that p is the only prime that ramifies in R_p; in general, the only primes in any R that can ramify are those dividing the discriminant of R. As mentioned previously, the ring R_n of integers in any cyclotomic field $K_n = \mathbb{Q}[e^{2\pi i/n}]$ coincides with $\mathbb{Z}[e^{2\pi i/n}]$. There is a slightly more complicated formula for the discriminant of R_n for general n.

I now shift gears, letting R be any Dedekind domain (that is, any integral domain integrally closed in its quotient field such that every ideal is finitely generated). I will show later that any nonzero ideal of R is uniquely a product of prime ideals; for now I take this property for granted and work out its consequences, following section 16.3 of the Dummit and Foote text. Let R be a a Dedekind domain, I a nonzero ideal of R.

Proposition 18, p. 768

If $I = P_1^{a_1} \cdots P_n^{a_n}$ with the P_i distinct prime ideals, then $R/I \cong S = R/P_1^{a_1} \times \cdots \times R/P_n^{a_n}$.

Proof.

Setting $I_i = P_i^{a_i}$, one sees that the I_i are pairwise coprime, so that $I_i + I_j = R$ for $i \neq j$; indeed, a prime ideal containing $I_i + I_j$ would have to contain both P_i and P_j and thus be all of R since P_i and P_j are maximal. Similarly, any two products of distinct I_i with no common terms are coprime, whence by a calculation done last quarter we have that the product $\prod I_i$ coincides with their intersection $\cap I_i$. Letting J_i be the product of the I_j with $j \neq i$ for all indices i, one checks that the sum of the J_j is not contained in any proper prime ideal so is all of R. Then for each i there is $a_i \in R$ with $a_i \equiv 1 \bmod I_i$ (that is, $a_i - 1 \in I_i$ and $a_i \equiv 0 \bmod I_j$ for $j \neq i$. Then the projection $R \to S$ sending r to the tuple $(\bar{r}, \ldots, \bar{r})$ of images of r in the quotients R/I_i is both injective and surjective, hence an isomorphism. $\square$

Corollary 19, p. 768

Every ideal of R/I is principal (though R/I need not be a principal ideal *domain*).

Proof.

By the proposition it is enough to show that every ideal of a quotient $R' = R/P^n$ is principal if P is a prime ideal of R. Since the ideals of R' are the images of ideals of R containing P^n, it follows that the image $\bar{P}$ of P is the only prime ideal of R' and every nonzero ideal of R' is a power of $\bar{P}$. Thus we are reduced to showing that $\bar{P}$ is principal. By unique factorization in R, we cannot have $P = P^2$, so choose $x \in P, x \notin P^2$. The only possible prime factorization of the ideal $(\bar{x})$ generated by the image of x in R' is then $\bar{P}$, whence $\bar{P}$ is principal, as desired. □