For large N, we see that $d_k \geqq (1/N)(\pi e^2/4)^N$.

We conclude by an example of which Artin was very fond. Consider the equation $f(X) = X^5 - X + 1$. The discriminant Δ of a root of $X^5 + aX + b$ is $5^5b^4 + 2^8a^5$. In this special case,

$$\Delta = 2869 = 19 \cdot 151.$$

Each prime factor occurs to the first power.

Let α be a root of $f(X)$ and $k = \mathbf{Q}(\alpha)$. Then α is integral over $\mathbf{Z}$. Since $f(X)$ is irreducible mod 5, it is irreducible over $\mathbf{Z}$ (or $\mathbf{Q}$) and k is of degree 5 over $\mathbf{Q}$. The discriminant of $\mathbf{Z}[\alpha]$ as a module over $\mathbf{Z}$ has no square factors. Hence it must be equal to $D(\mathfrak{o}_k)$, because it differs from $D(\mathfrak{o}_k)$ by a square. Hence $\mathbf{Z}[\alpha] = \mathfrak{o}_k$ by Proposition 10 of Chapter III, §3.

It is not difficult to show that the Galois group of the polynomial is the full symmetric group. Hence the splitting field K has degree 120 over $\mathbf{Q}$.

By the Minkowski theorem, every ideal class has an ideal $\mathfrak{b}$ such that $\mathbf{N}\mathfrak{b} < 4$ (using the value for the Minkowski constant in the table and trivial estimates). Since $\mathbf{N}\mathfrak{b}$ is an integer, it is either 1, 2, or 3. If $\mathbf{N}\mathfrak{b} \neq 1$, the only possibility is that $\mathfrak{b}$ is a prime ideal $\mathfrak{p}$ with $\mathbf{N}\mathfrak{p} = 2$ or 3. This would mean that the residue class field $\mathfrak{o}_k/\mathfrak{p}$ has degree 1 over $\mathbf{Z}/p\mathbf{Z}$ and hence that f has a root mod 2 or mod 3. This is impossible (direct computation), and hence the only possibility is that $\mathbf{N}\mathfrak{b} = 1$. But then $\mathfrak{b} = (1)$ and (oh miracle!) every ideal is principal. The ring of integers is a principal ideal ring.

As Artin noticed, it can be shown that the splitting field K is unramified over the extension $\mathbf{Q}(\sqrt{\Delta}) = \mathbf{Q}(\sqrt{19 \cdot 151})$.

Artin's example also gives an example of an unramified extension whose Galois group is the icosahedral group. As he once pointed out, given any Galois extension K of a number field k, with group G, there exist infinitely many finite extensions E of k such that $K \cap E = k$ and KE is unramified over E. To obtain such E, it suffices to construct an extension which absorbs locally all the ramification of K (this puts a finite number of conditions on E, which can be realized by the approximation theorem), and one must insure that $E \cap K = k$. To do this, one can for instance use the existence of primes and density theorems proved in a later chapter. We leave it as an exercise.

As a final application of the Minkowski theorem, we shall prove:

Theorem 5. *If k is a number field, denote by N_k and d_k the degree $[k : \mathbf{Q}]$ and absolute value of the discriminant respectively. Then the quotient $N_k/\log d_k$ is bounded for all $k \neq \mathbf{Q}$. Furthermore, there exists only a finite number of fields k having a given value of the discriminant.*

Proof. The first assertion follows from a trivial computation involving the inequality of the Corollary to Theorem 4, and the standard estimate