Zeitschrift: L'Enseignement Mathématique

Band: 34 (1988)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: EULER'S FAMOUS PRIME GENERATING POLYNOMIAL AND THE CLASS NUMBER OF IMAGINARY QUADRATIC FIELDS

Kapitel: C) Discriminant

Autor: Ribenboim, Paulo

DOI: https://doi.org/10.5169/seals-56587

If $d \equiv 1 \pmod 4$ then $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ is an integral basis of A.

C) Discriminant

Let $\{\alpha_1, \alpha_2\}$ be an integral basis. Then

$$D = D_K = \det \begin{pmatrix} \operatorname{Tr}(\alpha_1^2) & \operatorname{Tr}(\alpha_1\alpha_2) \\ \operatorname{Tr}(\alpha_1\alpha_2) & \operatorname{Tr}(\alpha_2^2) \end{pmatrix}$$

is independent of the choice of the integral basis. It is called the discriminant of K. It is a non-zero integer.

If $d \equiv 2$ or $3 \pmod 4$ then

$$D = \det \begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\sqrt{d}) \\ \operatorname{Tr}(\sqrt{d}) & \operatorname{Tr}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} \quad \text{so } D = 4d\,.$$

If $d \equiv 1 \pmod 4$ then

$$D = \det \begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}\left(\dfrac{1+\sqrt{d}}{2}\right) \\ \operatorname{Tr}\left(\dfrac{1+\sqrt{d}}{2}\right) & \operatorname{Tr}\left(\dfrac{1+\sqrt{d}}{2}\right)^2 \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \dfrac{1+d}{2} \end{pmatrix} \quad \text{so} \quad D = d\,.$$

Every discriminant is $D \equiv 0$ or $1 \pmod 4$.

In terms of the discriminant,

$$A = \left\{ \frac{a + b\sqrt{D}}{2} \;\middle|\; a, b \in \mathbf{Z}, \quad a^2 \equiv Db^2 \pmod 4 \right\}.$$

D) Decomposition of primes

Let $K = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer, let A be the ring of integers of K.

The ideal $P \neq 0$ of A is a prime ideal if the residue ring A/P has no zero-divisors.

If P is a prime ideal there exists a unique prime number p such that $P \cap \mathbf{Z} = \mathbf{Z}p$, or equivalently, $P \supseteq Ap$.