Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de 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

Autor: Ribenboim, Paulo

Kapitel: B) Rings of integers

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

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 15.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Conversely, if K is a field, which is a quadratic extension of $\mathbf{Q}$, then it is necessarily of the form $K = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer.

If $d > 0$ then K is a subfield of the field $\mathbf{R}$ of real numbers: it is called a real quadratic field.

If $d < 0$ then K is not a subfield of $\mathbf{R}$, and it is called an imaginary quadratic field.

If $\alpha = a + b\sqrt{d} \in K$, with $a, b \in \mathbf{Q}$, its conjugate is $\alpha' = a - b\sqrt{d}$. Clearly, $\alpha = \alpha'$ exactly when $\alpha \in \mathbf{Q}$.

The norm of α is $N(\alpha) = \alpha\alpha' = a^2 - db^2 \in \mathbf{Q}$. It is obvious that $N(\alpha) \neq 0$ exactly when $\alpha \neq 0$. If $\alpha, \beta \in K$ then $N(\alpha\beta) = N(\alpha)\, N(\beta)$; in particular, if $\alpha \in \mathbf{Q}$ then $N(\alpha) = \alpha^2$.

The trace of α is $\mathrm{Tr}(\alpha) = \alpha + \alpha' = 2a \in \mathbf{Q}$. If $\alpha, \beta \in K$ then $\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$; in particular, if $\alpha \in \mathbf{Q}$ then $\mathrm{Tr}(\alpha) = 2\alpha$.

It is clear that α, α' are the roots of the quadratic equation $X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) = 0$.

B) Rings of integers

Let $K = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer.

$\alpha \in K$ is an algebraic integer when there exist integers $m, n \in \mathbf{Z}$ such that $\alpha^2 + m\alpha + n = 0$.

Let A be the set of all algebraic integers of K. A is a subring of K, which is the field of fractions of A, and $A \cap \mathbf{Q} = \mathbf{Z}$. If $\alpha \in A$ then the conjugate $\alpha' \in A$. Clearly, $\alpha \in A$ if and only if both $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ are in $\mathbf{Z}$.

Here is a criterion for the element $\alpha = a + b\sqrt{d}$ $(a, b \in \mathbf{Q})$ to be an algebraic integer: $\alpha \in A$ if and only if

$$\begin{cases} 2a = u \in \mathbf{Z}, \quad 2b = v \in \mathbf{Z} \\ u^2 - d\,v^2 \equiv 0 \pmod 4. \end{cases}$$

Using this criterion, it may be shown:

If $d \equiv 2$ or $3 \pmod 4$ then $A = \{a + b\sqrt{d} \mid a, b \in \mathbf{Z}\}$.

If $d \equiv 1 \pmod 4$ then $A = \left\{\dfrac{a + b\sqrt{d}}{2} \,\middle|\, a, b \in \mathbf{Z}, a \equiv b \pmod 2\right\}$.

If $\alpha_1, \alpha_2 \in A$ are such that every element $\alpha \in A$ is uniquely of the form $\alpha = m_1\alpha_1 + m_2\alpha_2$, with $m_1, m_2 \in \mathbf{Z}$, then $\{\alpha_1, \alpha_2\}$ is called an integral basis of A. In other words, $A = \mathbf{Z}\alpha_1 \oplus \mathbf{Z}\alpha_2$.

If $d \equiv 2$ or $3 \pmod 4$ then $\{1, \sqrt{d}\}$ is an integral basis of A.

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

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

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

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

If $d \equiv 1 \pmod 4$ then

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

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, $P \supseteq Ap$.