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: D) Decomposition of primes

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, $P \supseteq Ap$.

If I, J are non-zero ideals of A, it is said that I divides J when there exists an ideal I_1 of A such that $I \,.\, I_1 = J$.

The prime ideal P containing the prime number p divides the ideal Ap.

If I is a non-zero ideal of A then the residue ring A/I is finite. The norm of I is $N(I) = \#(A/I)$.

Properties of the norm:

If I, J are non-zero ideals, then $N(I \,.\, J) = N(I)\, N(J)$.
If I divides J then $N(I)$ divides $N(J)$.
If $\alpha \in A$, $\alpha \neq 0$, then $N(A\alpha) = |\, N(\alpha) \,|$ (absolute value of the norm of α). In particular, if $a \in \mathbf{Z}$ then $N(Aa) = a^2$.
If the prime ideal P divides Ap then $N(P)$ is equal to p or to p^2.

Every ideal $I \neq 0$ is, in unique way, the product of powers of prime ideals:

$$I = \prod_{i=1}^{n} P_i^{e_i} .$$

If I, J are non-zero ideals, if $I \supseteq J$ then I divides J.

Every ideal $I \neq 0$ may be generated by two elements, of which one may be chosen in $\mathbf{Z}$; if $I \cap \mathbf{Z} = \mathbf{Z}n$ then $I = An + A\alpha$ for some $\alpha \in A$. In this case, the following notation is used: $I = (n, \alpha)$.

Consider now the special case where p is a prime number. Then Ap is of one of the following types:

$$\begin{cases} Ap = P^2\,, & \text{where } P \text{ is a prime ideal: } p \text{ is ramified in } K. \\ Ap = P\,, & \text{where } P \text{ is a prime ideal: } p \text{ is inert in } K. \\ Ap = P_1 P_2\,, & \text{where } P_1, P_2 \text{ are distinct prime ideals: } p \text{ is decomposed or splits in } K. \end{cases}$$

Note also that if $Ap = I \,.\, J$, where I, J are any ideals (different from A), not necessarily distinct, then I, J must in fact be prime ideals.

I shall now indicate when a prime number p is ramified, inert or decomposed, and also give generators of the prime ideals of A. There are two cases: $p \neq 2$, $p = 2$.

Denote by $\left(\dfrac{d}{p}\right)$ the Legendre symbol, so

$$\begin{cases} \left(\dfrac{d}{p}\right) = 0 & \text{when } p \text{ divides } d\,, \\ \left(\dfrac{d}{p}\right) = +\,1 & \text{when } d \text{ is a square modulo } p\,, \\ \left(\dfrac{d}{p}\right) = -\,1 & \text{when } d \text{ is not a square modulo } p\,. \end{cases}$$

Let $p \neq 2$.

1) If p divides d then $Ap = (p, \sqrt{d})^2$.

2) If p does not divide d and there does not exist $a \in \mathbf{Z}$ such that $d \equiv a^2 \pmod{p}$ then Ap is a prime ideal.

3) If p does not divide d and there exists $a \in \mathbf{Z}$ such that $d \equiv a^2 \pmod{p}$ then $Ap = (p, a+\sqrt{d})\,(p, a-\sqrt{d})$.

Hence

1) p is ramified if and only if $\left(\frac{d}{p}\right) = 0$.

2) p is inert if and only if $\left(\frac{d}{p}\right) = -1$.

3) p is decomposed if and only if $\left(\frac{d}{p}\right) = +1$.

Proof. The proof is divided into several parts.

a) If $\left(\frac{d}{p}\right) = -1$ then Ap is a prime ideal.

Otherwise $Ap = P \,.\, P'$ or P^2, with $P \cap \mathbf{Z} = \mathbf{Z}p$. Let $\alpha \in A$ be such that $P = (p, \alpha) \supseteq A\alpha$ so $P \mid A\alpha$, hence p divides $N(P)$, which divides $N(A\alpha) = |N(\alpha)|$. If $p \mid \alpha$ then $\frac{\alpha}{p} \in A$ and $P = Ap \,.\, \left(1, \frac{\alpha}{p}\right) = Ap$, which is absurd. So $p \nmid \alpha$. Then,

$$\left\{\begin{array}{l} d \equiv 2 \text{ or } 3 \pmod{4} \\ \\ d \equiv 1 \pmod{4} \end{array}\right. \Rightarrow \left\{\begin{array}{ll} \alpha = a + b\sqrt{d}, & \text{with} \quad a, b \in \mathbf{Z} \\ \\ \alpha = \dfrac{a + b\sqrt{d}}{2}, & \text{with} \quad a, b \in \mathbf{Z}, \quad a \equiv b \pmod{2} \end{array}\right.$$

$$\Rightarrow \left\{\begin{array}{l} N(\alpha) = a^2 - db^2 \\ \\ N(\alpha) = \dfrac{a^2 - db^2}{4} \end{array}\right. \Rightarrow \quad p \text{ divides } a^2 - db^2,$$

hence $a^2 \equiv db^2 \pmod{p}$ and so $p \nmid b$ (otherwise $p \mid a$, hence $p \mid \alpha$, which is absurd).

Let b' be such that $bb' \equiv 1 \pmod{p}$, so $(ab')^2 \equiv d \pmod{p}$, therefore either $p \mid d$ or $\left(\frac{d}{p}\right) = +1$, which is a contradiction.

b) If $\left(\frac{d}{p}\right) = 0$ then $Ap = (p, \sqrt{d})^2$.

Indeed, let $P = (p, \sqrt{d})$, so $P^2 = (p^2, p\sqrt{d}, d) = Ap\left(p, \sqrt{d}, \frac{d}{p}\right)$ since $\frac{d}{p} \in \mathbf{Z}$. But d is square-free, so $gcd\left(p, \frac{d}{p}\right) = 1$, hence $P^2 = Ap$ and this implies that P is a prime ideal.

c) If $\left(\frac{d}{p}\right) = -1$ then $Ap = (p, a+\sqrt{d})\,(p, a-\sqrt{d})$, where $1 \leqslant a \leqslant p-1$ and $a^2 \equiv d \pmod{p}$.

Indeed,

$$(p, a+\sqrt{d})\,(p, a-\sqrt{d}) = (p^2, pa+p\sqrt{d}, pa-p\sqrt{d}, a^2-d)$$

$$= Ap\left(p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p}\right) = Ap\left(p, a+\sqrt{d}, a-\sqrt{d}, 2a, \frac{a^2-d}{p}\right) = Ap\,,$$

because $gcd(p, 2a) = 1$. If one of the ideals $(p, a+\sqrt{d})$, $(p, a-\sqrt{d})$ is equal to A, so is the other which is not possible.

So $(p, a+\sqrt{d})$, $(p, a-\sqrt{d})$ are prime ideals. They are distinct: if $(p, a+\sqrt{d}) = (p, a-\sqrt{d})$ then they are equal to their sum

$$(p, a+\sqrt{d}, a-\sqrt{d}) = (p, a+\sqrt{d}, a-\sqrt{d}, 2a) = A\,,$$

which is an absurd.

Finally, these three cases are exclusive and exhaustive, so the converse assertions are also true. □

Note. If $d \equiv 1 \pmod 4$ and $d \equiv a^2 \pmod p$ then

$$(p, a+\sqrt{d}) = \big(p, l(a-1)+\omega\big)\,,$$

where $\omega = \dfrac{1+\sqrt{d}}{2}$ and $2l \equiv 1 \pmod p$. Hence, if $\left(\frac{d}{p}\right) \neq -1$ there exists $b \in \mathbf{Z}$, $0 \leqslant b \leqslant p-1$, such that p divides $N(b+\omega)$ and moreover if $b = p-1$ then $d \equiv 1 \pmod p$.

Indeed, $a + \sqrt{d} = a - 1 + 2\omega$. If $2l \equiv 1 \pmod p$ then

$$(p, a+\sqrt{d}) = \big(p, (a-1)+2\omega\big) = \big(p, l(a-1)+\omega\big)\,.$$

If $\left(\frac{d}{p}\right) \neq -1$ then there exists a prime ideal P dividing Ap, where

$$P = (p, a+\sqrt{d}), 0 \leqslant a \leqslant p-1 .$$

So $P = (p, b+\omega)$ with $0 \leqslant b \leqslant p-1$, $b \equiv l(a-1) \pmod{p}$.

Since $P \supseteq A(b+\omega)$ then p divides $N(P)$, which divides $N(b+\omega)$. Finally, if p divides $N(p-1+\omega) = N\left(\dfrac{2p-1+\sqrt{d}}{2}\right) = \dfrac{(2p-1)^2 - d}{4}$ then p divides $\dfrac{1-d}{4}$ so $d \equiv 1 \pmod{p}$.

Let $p = 2$.

If $d \equiv 2 \pmod 4$ then $A2 = (2, \sqrt{d})^2$.
If $d \equiv 3 \pmod 4$ then $A2 = (2, 1+\sqrt{d})^2$.
If $d \equiv 1 \pmod 8$ then $A2 = (2, \omega)(2, \omega')$.
If $d \equiv 5 \pmod 8$ then $A2$ is a prime ideal.

Hence

1) 2 is ramified if and only if $d \equiv 2$ or $3 \pmod 4$.

2) 2 is inert if and only if $d \equiv 5 \pmod 8$.

3) 2 is decomposed if and only if $d \equiv 1 \pmod 8$.

Proof. The proof is divided into several parts.

a) If $d \equiv 5 \pmod 8$ then $A2$ is a prime ideal.

Otherwise, $A2 = P \,.\, P'$ or P^2, with $P \cap \mathbf{Z} = \mathbf{Z}2$. Then there exists $\alpha \in A$ such that $P = (2, \alpha) \supseteq A\alpha$, so P divides $A\alpha$ and 2 divides $N(P)$, which divides $N(\alpha)$.

If $2 \mid \alpha$ then $P = A2\left(l, \dfrac{\alpha}{2}\right) = A2$, which is absurd. Thus

$$2 \not\mid \alpha = \frac{a + b\sqrt{d}}{2}, \quad \text{with} \quad a \equiv b \pmod 2, \quad \text{so} \quad N(\alpha) = \frac{a^2 - db^2}{4}.$$

From $2 \mid N(\alpha)$ then 8 divides $a^2 - db^2 \equiv a^2 - 5b^2 \equiv a^2 + 3b^2 \pmod 8$.

If a, b are odd then $a^2 \equiv b^2 \equiv 1 \pmod 8$, so $a^2 + 3b^2 \equiv 4 \pmod 8$, which is absurd. So a, b are even, $a = 2a'$, $b = 2b'$, and $\alpha = a' + b'\sqrt{d}$, 2 divides $N(\alpha) = a'^{\,2} - db'^{\,2}$.

Since d is odd, then a', b' are both even or both odd.

If a', b' are even then 2 divides α, which is absurd.

If a', b' are odd then $\alpha = a' + b'\sqrt{d} =$ (multiple of 2) $+ 1 + \sqrt{d}$ $=$ (multiple of 2) $+ 2\omega =$ (multiple of 2), which is absurd.

b) If $d \equiv 1 \pmod 8$ then $A2 = (2, \omega)(2, \omega')$.

Indeed,

$$(2, \omega)(2, \omega') = \left(4, 2\omega, 2\omega', \frac{1-d}{4}\right) = A2\left(2, \omega, \omega', \frac{1-d}{8}\right) = A2\,,$$

because $\omega + \omega' = 1$.

Also $(2, \omega) \neq (2, \omega')$, otherwise these ideals are equal to their sum $(2, \omega, \omega') = A$, because $\omega + \omega' = 1$.

c) If $d \equiv 2$ or $3 \pmod 4$ then $A2 = (2, \sqrt{d})^2$, respectively $(2, 1+\sqrt{d})^2$. First let $d = 4e + 2$ then

$$(2, \sqrt{d})^2 = (4, 2\sqrt{d}, d) = A2(2, \sqrt{d}, 2e+1) = A2\,,$$

so $(2, \sqrt{d})$ is a prime ideal.

Now, let $d = 4e + 3$, then

$$(2, 1+\sqrt{d})^2 = (4, 2+2\sqrt{d}, 1+d+2\sqrt{d}) = (4, 2+2\sqrt{d}, 4(e+1)+2\sqrt{d})$$
$$= A2(2, 1+\sqrt{d}, 2(e+1)+\sqrt{d}) = A2(2, 2e+1, 1+\sqrt{d}, 2(e+1)+\sqrt{d}) = A2$$

and so $(2, 1+\sqrt{d})$ is a prime ideal.

Finally, these three cases are exclusive and exhaustive, so the converse assertions also hold. □

E) Units

The element $\alpha \in A$ is a unit if there exists $\beta \in A$ such that $\alpha\beta = 1$. The set U of units is a group under multiplication. Here is a description of the group of units in the various cases. First let $d < 0$.

Let $d \neq -1, -3$. Then $U = \{\pm 1\}$.

Let $d = -1$. Then $U = \{\pm 1, \pm i\}$, with $i = \sqrt{-1}$.

Let $d = -3$. Then $U = \{\pm 1, \pm \rho, \pm \rho^2\}$, with $\rho^3 = 1$, $\rho \neq 1$, i.e. $\rho = \dfrac{-1+\sqrt{-3}}{2}$.

Let $d > 0$. Then the group of units is the product $U = \{\pm 1\} \times C$, where C is a multiplicative cyclic group. Thus $C = \{\varepsilon^n \mid n \in \mathbf{Z}\}$, where ε is the smallest unit such that $\varepsilon > 1$. ε is called the fundamental unit.