5–10 July 2004, Antalya, Turkey — Dynamical Systems and Applications, Proceedings, pp. 443–449

Decomposition of Prime Ideals in the Extensions

B. Kendirli
Department of Mathematics, Fatih University,
Istanbul, Turkey
E-mail: bkendirli@fatih.edu.tr

Abstract

The factorization of primes in abelian extensions are examined by examples and remarks are given concerning the extension to nonabelian field extensions.

Key words: Factorization, Class field theory.

1 Introduction

Let us try to solve the equation $p = x^2 + y^2$ in integers for a given prime integer p. It is easily seen that $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$. But we cannot find integers x and y such that $7 = x^2 + y^2$ or $11 = x^2 + y^2$. In fact, it is known that if $p = 2$ or $p \equiv 1 \pmod 4$, then $p = x^2 + y^2$ has solutions but if $p \equiv 3 \pmod 4$, there exists no solution. In complex numbers: $2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$, $5 = (2 + \sqrt{-1})(2 - \sqrt{-1})$, $13 = (3 + 2\sqrt{-1})(3 - 2\sqrt{-1})$, $17 = (4 + \sqrt{-1})(4 - \sqrt{-1})$ are clear. But we cannot find similiar expression for 7 and 11. Hence we are trying to factorize the prime integers in the ring of integers $\mathbb{Z}\left[\sqrt{-1}\right]$ of the field $\mathbb{Q}(\sqrt{-1})$. $1 + \sqrt{-1}$, $2 + \sqrt{-1}$, $2 - \sqrt{-1}$, $3 + 2\sqrt{-1}$, $3 - 2\sqrt{-1}$, $4 + \sqrt{-1}$, $4 - \sqrt{-1}$ are prime integers in $\mathbb{Z}\left[\sqrt{-1}\right]$. We observe that the factorization of p in $\mathbb{Z}\left[\sqrt{-1}\right]$ is equivalent to finding integer solutions x, y of the equation $p = x^2 + y^2$. In fact, in general finding the integer solutions of the equation $n = x^2 + y^2$ can be reduced to the factorization of n in $\mathbb{Z}\left[\sqrt{-1}\right]$ for an arbitrary integer n. In fact, as it is well known if $n = s^2 m$, m a square free integer, m has only prime factors $p = 2$ or $p \equiv 1 \pmod 4$ if and only if the equation $n = x^2 + y^2$ has integer solutions x and y.

Now let us look at $p = x^2 + 2y^2$. We can see immediately that $3 = 1^2 + 2 \cdot 1^2$, $11 = 3^2 + 2 \cdot 1^2$, $17 = 3^2 + 2 \cdot 2^2$. In other words, $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$, $11 = (3 + \sqrt{-2})(3 - \sqrt{-2})$, $17 = (3 + 2\sqrt{-2})(3 - 2\sqrt{-2})$. Hence the solutions of the equation $p = x^2 + 2y^2$ can be reduced to the factorization of p in $\mathbb{Z}\left[\sqrt{-2}\right]$. In fact, $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$ is a necessary and sufficient condition.

Now let us look at $p = x^2 - 2y^2$. $7 = 3^2 - 2 \cdot 1^2$, $17 = 5^2 - 2 \cdot 2^2$, $23 = 5^2 - 2 \cdot 1^2$ are obvious. In other words, $7 = \left(3 + \sqrt{2}\right)\left(3 - \sqrt{2}\right)$, $17 = \left(5 + 2\sqrt{2}\right)\left(5 - 2\sqrt{2}\right)$,

$23 = (5+\sqrt{2})(5-\sqrt{2})$ in $\mathbb{Z}\left[\sqrt{2}\right]$. In fact, $p \equiv 1 \pmod 8$ or $p \equiv 7 \pmod 8$ is a necessary and sufficient condition for the existence of integer solutions x, y of $p = x^2 - 2y^2$.

In general, the integer solutions of $n = ax^2 + bxy + cy^2$ for given integers a, b, c, n can be obtained as follows. Calculate the discriminant $D = b^2 - 4ac$. If $D = s^2$ for some integer s, then it can be solved easily. If $D = s^2 d$, where d is a square-free integer, then we look at the factorization of $na = \left(ax + \frac{b+s\sqrt{d}}{2}y\right)\left(ax + \frac{b-s\sqrt{d}}{2}y\right)$ in the ring of integers I_d of $\mathbb{Q}\left(\sqrt{d}\right)$. For instance, if $65 = x^2 + 3xy - 5y^2$, then $D = 3^2 + 4 \cdot 5 = 29$. Therefore $s = 1$, $d = 29$. Hence we can obtain the solutions $65 = 7^2 + 3 \cdot 7 \cdot 1 - 5 \cdot 1^2$, $65 = 10^2 + 3 \cdot 10 \cdot (-1) - 5(-1)^2$, $65 = 10^2 + 3 \cdot 10 \cdot 7 - 5 \cdot 7^2$, $65 = 31^2 + 3 \cdot 31 \cdot (-7) - 5 \cdot (-7)^2$ from the factorization of $65 = x^2 + 3xy - 5y^2 = \left(x + \frac{3+\sqrt{29}}{2}y\right)\left(x + \frac{3-\sqrt{29}}{2}y\right)$ in the ring of integers I_{29} of $\mathbb{Q}(\sqrt{29})$. After that we can obtain all other infinitely many solutions by a simple formula.

As we observe from the above examples the factorization of a prime integer p in $\mathbb{Q}\left(\sqrt{-1}\right)$, $\mathbb{Q}\left(\sqrt{-2}\right)$, $\mathbb{Q}\left(\sqrt{2}\right)$ or, in general, in $\mathbb{Q}\left(\sqrt{d}\right)$ is equivalent to the following fact: Find a divisor α of p in I_d such that p is equal to the product of α and the conjugate of α. If we define the Norm function on $\mathbb{Q}\left(\sqrt{d}\right)$ as $N(a + b\sqrt{d}) = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right)$, then we can interpret the fact of factorization as finding the image of I_d under the Norm function:

$$\begin{aligned}
5 = \left(2+\sqrt{-1}\right)\left(2-\sqrt{-1}\right) &\iff 5 = N(2+\sqrt{-1}),\\
13 = \left(2+3\sqrt{-1}\right)\left(2-3\sqrt{-1}\right) &\iff 13 = N\left(2+3\sqrt{-1}\right),\\
7 = \left(2+\sqrt{-3}\right)\left(2-\sqrt{-3}\right) &\iff 7 = N\left(2+\sqrt{-3}\right),\\
65 = 7^2 + 3 \cdot 7 \cdot 1 - 5 \cdot 1^2 &\iff 65 = N\left(7 + \frac{3+\sqrt{29}}{2} \cdot 1\right).
\end{aligned}$$

2 Factorization of ideals

Let us look at the situation in $\mathbb{Q}\left(\sqrt{-5}\right)$. Here we do not have a unique factorization as $6 = 2 \cdot 3 = (1+\sqrt{-5})\left(1-\sqrt{-5}\right)$. But the factorization of ideals is unique. $6\mathbb{Z}[\sqrt{-5}] = 2\mathbb{Z}[\sqrt{-5}]3\mathbb{Z}[\sqrt{-5}] = (\left(2, 1+\sqrt{-5}\right)^2)(\left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right))$ and

$$\begin{aligned}
6\mathbb{Z}[\sqrt{-5}] &= \left(1+\sqrt{-5}\right)\mathbb{Z}[\sqrt{-5}]\left(1-\sqrt{-5}\right)\mathbb{Z}[\sqrt{-5}]\\
&= (\left(2, 1+\sqrt{-5}\right)\left(3, 1+\sqrt{-5}\right))(\left(2, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right))
\end{aligned}$$

as factorizations of prime ideals are unique. It is known that if the class number of $\mathbb{Q}\left(\sqrt{d}\right)$ is 1, we have the unique factorization in I_d. If not, we do not have a unique factorization of elements in I_d but we have a unique factorization of ideals in I_d.

3 The relation of factorization with the solutions of quadratic equations

It is known that the ideal generated by a prime p which is different from 2 and does not divide d, is a product of two prime ideals if and only if $x^2 \equiv d \pmod{p}$ has integer solutions, *i.e.*, $x^2 - d$ is factorizable in the finite field $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. **In fact, it is generally true that a factorization of an unramified ideal in an abelian extension corresponds to the factorizaton of a polynomial in a finite field**. For instance, 2 is a solution of $x^2 \equiv -5 \pmod{3}$, therefore $3\mathbb{Z}[\sqrt{-5}] = \left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right)$ is written as a product of prime ideals. On the other hand, since there is no integer satisfying $x^2 \equiv -5 \pmod{11}$, the ideal $11\mathbb{Z}[\sqrt{-5}]$ cannot be factorized in $\mathbb{Z}[\sqrt{-5}]$ but it is still prime.

It is known that for a prime p, $ax^2 + bx + c \equiv 0 \pmod{p}$ can be reduced to the equation $x^2 \equiv d \pmod{p}$, hence its solution depends on the factorization of the ideal generated by p in I_d. The solutions of $ax^2 + bx + c \equiv d \pmod{p^m}$ can be obtained from the solutions of $ax^2 + bx + c \equiv 0 \pmod{p}$. The general case $ax^2 + bx + c \equiv 0 \pmod{n}$ for $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ can be obtained from the solutions of $ax^2+bx+c \equiv 0 \pmod{p_i^{m_i}}$ for $i = 1, 2, \ldots, k$ by the Chinese remainder theorem. Of course, it is essential for the study of solutions of the quadratic equation $ax^2 + bx + c = 0$.

Now let us take two distinct prime integers p and q different from 2. The factorization of the ideal generated by p in $\mathbb{Q}\left(\sqrt{q}\right)$ is closely connected with the factorization of the ideal generated by q in $\mathbb{Q}\left(\sqrt{p}\right)$ and, in fact, it is expressed as the quadratic reciprocity law $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$.

4 The case of cyclotomic field extension

Let us look at the factorization of the ideal generated by a prime integer p in the ring of integers $\mathbb{Z}\left[e^{2\pi i/16}\right]$ of $\mathbb{Q}(e^{2\pi i/16})$.

$2\mathbb{Z}\left[e^{2\pi i/16}\right] = \left((1 - e^{2\pi i/16})\mathbb{Z}\left[e^{2\pi i/16}\right]\right)^8$ as the 8th power of a single prime ideal,

$7\mathbb{Z}\left[e^{2\pi i/16}\right] = A_1A_2$ as the product of two prime ideals since $\overline{\mathrm{Irr}(e^{2\pi i/16}, \mathbb{Q})(x)} = \overline{x^8 + 1} \pmod{7}$ can be factorized as the product of two irreducible polynomials in $\mathbb{Z}_7$,

$31\mathbb{Z}\left[e^{2\pi i/16}\right] = B_1B_2$ as the product of two prime ideals,

$3\mathbb{Z}\left[e^{2\pi i/16}\right] = C_1C_2C_3C_4$ as the product of four prime ideals,

$5\mathbb{Z}\left[e^{2\pi i/16}\right] = D_1D_2D_3D_4$ as the product of four prime ideals, and

$17\mathbb{Z}\left[e^{2\pi i/16}\right] = E_1E_2E_3E_4E_5E_6E_7E_8$ as the product of 8 prime ideals, can be verified easily. Hence if the prime integer p is different from 2, then the ideal generated by p is the product of 2 or 4 or 8 prime ideals in $\mathbb{Z}\left[e^{2\pi i/16}\right]$.

5 General case

If the prime integer p does not divide n, then the ideal generated by p in the ring of integers $\mathbb{Z}\left[e^{2\pi i/n}\right]$ of $\mathbb{Q}\left(e^{2\pi i/n}\right)$ can be factorized as $\phi(n)/f$ different prime ideals. Here ϕ is the Euler function and f is the least positive integer satisfying the congruence equation $p^f \equiv 1 \pmod{n}$. $f = 2$ if $n = 16,\ p = 7,\ \ f = 4$ if $n = 16,\ p = 3$ and $f = 1$ if $n = 16,\ p = 17$.

In particular, the ideal generated by p is a product of $\phi(n)$ (which is equal to the degree of the extension) distinct prime ideals if and only if $p \equiv 1 \pmod{n}$.

In such a case where the degree of extension is equal to the number of factors we say that p splits completely in the ring of integers of the extension. Let us denote by $\mathrm{Sp}(\mathbb{K}/\mathbb{Q})$ the set of all prime integers whose ideal splits completely in the ring of integers of $\mathbb{K}$. Then the following table is clear:

$\mathbb{K}$	$\mathrm{Sp}(\mathbb{K}/\mathbb{Q})$
$\mathbb{Q}\left(\sqrt{-1}\right)$	$p \equiv 1 \pmod{4}$
$\mathbb{Q}\left(\sqrt{2}\right)$	$p \equiv 1 \pmod{8}$ and $p \equiv 7 \pmod{8}$
$\mathbb{Q}\left(\sqrt{-2}\right)$	$p \equiv 1 \pmod{8}$ and $p \equiv 3 \pmod{8}$
$\mathbb{Q}\left(e^{2\pi i/16}\right)$	$p \equiv 1 \pmod{16}$
$\mathbb{Q}\left(e^{2\pi i/n}\right)$	$p \equiv 1 \pmod{n}$

Now we can ask the following important question: **Which subsets of the set of prime integers can be $\mathrm{Sp}(\mathbb{K}/\mathbb{Q})$ for a finite Galois extension $\mathbb{K}$ of $\mathbb{Q}$?** We can find the answer by defining Frobenius automorphism with the class field theory.

Example 1 Obviously $G\left(\mathbb{Q}\left(\sqrt{-1}\right)/\mathbb{Q}\right) = \{x + yi \longmapsto x + yi,\ x + yi \longmapsto x - yi\}$. Here $2 = -i(1+i)^2$ is a ramified prime but all other prime integers are unramified. There exists an automorphism Fr_p in $\mathbb{Q}\left(\sqrt{-1}\right)$ such that $\mathrm{Fr}_p(x+yi) \equiv (x+yi)^p \pmod{p} \forall x, y \in \mathbb{Z}$ for a given prime integer p. It is called the Frobenius automorphism corresponding to the unramified prime p.

$\mathrm{Fr}_3(x+yi) \equiv (x+yi)^3 \pmod{3}$ can be calculated by $(x+yi)^3 \equiv x^3 + \binom{3}{1}x^2yi + \binom{3}{2}x(yi)^2 + (yi)^3 \equiv x^3 - y^3i \equiv x - yi \pmod{3}$ as $\mathrm{Fr}_3(x+yi) = x - yi$.

$\mathrm{Fr}_5(x+yi) \equiv (x+yi)^5 \pmod{(2+i)}$, $(x+yi)^5 \equiv x^5 + \binom{5}{1}x^4yi + \binom{5}{2}x^3(yi)^2 + \cdots + (yi)^5 \equiv x^5 + y^5i \equiv x + yi \pmod{(2+i)} \Longrightarrow \mathrm{Fr}_5(x+yi) = x + yi$.

In fact, it is known that Fr_p is the identity automorphism if and only if $p \equiv 1 \pmod 4$ and $\mathrm{Fr}_p(x+yi) = x - yi$ if and only if $p \equiv 3 \pmod 4$. In terms of factorization we can say that

Fr_p is identity $\Longleftrightarrow p$ splits completely in $\mathbb{Q}\left(\sqrt{-1}\right)$, $\mathrm{Fr}_p(x+yi) = (x-yi) \Longleftrightarrow p$ remains prime in $\mathbb{Z}\left[\sqrt{-1}\right]$.

Now let a and b be integers different from 2. If $a = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, $b = q_1^{n_1} q_2^{n_2} \cdots q_l^{n_l}$, then we define $\mathrm{Ar}_{a/b}$ as the composition of Frobenius automorphisms corresponding to the primes. $\mathrm{Ar}_{a/b}$ is an onto map from $\{(a/b)\mathbb{Z} :\ a$ and b are odd integers$\}$ to $G\left(\mathbb{Q}\left(\sqrt{-1}\right)/\mathbb{Q}\right)$. The kernel of Ar is $\mathrm{Ker(Ar)} = \{(a/b)\mathbb{Z} :\ a$ and b are odd integers, the number of prime integers which are 3 modulo 4 and which divide a or b is even$\}$ or in brief $\mathrm{Ker(Ar)} = \{(a/b)\mathbb{Z} :\ a$ and b are odd integers and $a \equiv b \pmod 4\}$. For instance, $5, 13, 17, 49, 77 = 7 \cdot 11$ are in Ker(Ar). The most important property of Ker(Ar) is that $\mathrm{Sp}\left(\mathbb{Q}\left(\sqrt{-1}\right)/\mathbb{Q}\right) = \{p :\ p$ is prime and $p \equiv 1 \pmod 4\} = \{p :\ p$ is prime and $p \in \mathrm{Ker(Ar)}\}$. Another property of Ker(Ar) is that it is generated by $\mathbb{Q}_{(4)\infty,1} = \{(1+4a/b)\mathbb{Z} :\ 1+4a/b$ is a positive integer and b is an odd integer$\}$ and the group
$N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathbb{Z}[\sqrt{-1}]) = \{N(x+yi)\mathbb{Z} :\ x, y \in \mathbb{Z}\} = \{n\mathbb{Z} :\ n = x^2 + y^2,\ x, y \in \mathbb{Z}\}$. The most important property is that $\mathbb{Q}_{(4)\infty,1} \subseteq \mathrm{Ker(Ar)} \subseteq I_{(4)}$. Here the symbol ∞ points out that the extension of $\mathbb{Q}$ is a nonreal complex extension, hence the numbers of the form $1 + 4a/b$ are positive.

Example 2 $G\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right) = \{x + y\sqrt{2} \longmapsto x + y\sqrt{2},\ x + y\sqrt{2} \longrightarrow x - y\sqrt{2}\}$. 2 is the only ramified prime.

We can define Frobenius automorphisms for odd prime integers.

$\mathrm{Fr}_3(x+y\sqrt{2}) \equiv (x+y\sqrt{2})^3 \pmod 3$, $(x+y\sqrt{2})^3 \equiv x^3 + 2\sqrt{2}y^3 \equiv x - y\sqrt{2} \pmod 3 \Longrightarrow \mathrm{Fr}_3(x+y\sqrt{2}) = x - y\sqrt{2}$.

$\mathrm{Fr}_7(x+y\sqrt{2}) \equiv (x+y\sqrt{2})^7 \equiv x^7 + 8\sqrt{2}y^7 \equiv x + \sqrt{2}y \pmod{(3+\sqrt{2})} \Longrightarrow \mathrm{Fr}_7(x+y\sqrt{2}) \equiv (x+y\sqrt{2})$. In fact, the following is true:

$p \equiv 1$ or $7 \pmod 8 \Longleftrightarrow \mathrm{Fr}_p$ is identity $\Longleftrightarrow p$ splits completely in $\mathbb{Z}\left[\sqrt{2}\right]$.

$p \equiv 3$ or $5 \pmod 8 \Longleftrightarrow \mathrm{Fr}_p(x+y\sqrt{2}) = x - y\sqrt{2} \Longleftrightarrow p$ remains prime in $\mathbb{Z}\left[\sqrt{2}\right]$.

$\mathrm{Ker(Ar)} = \{(a/b)\mathbb{Z} :\ a$ and b are odd integers and the number of prime factors of a and b of the form $p \equiv 3$ or $5 \pmod 8$ is even$\}$.

$\mathbb{Q}_{(8),1} = \{(1+8c/d)\mathbb{Z} :\ d$ is an odd integer $\} \subseteq \mathrm{Ker(Ar)} \subseteq I_{(8)} = \{(a/b)\mathbb{Z} :\ a, b$ are odd integers$\}$.

Example 3 $G\left(\mathbb{Q}\left(\sqrt{-5}\right)/\mathbb{Q}\right) = \{x + y\sqrt{-5} \longrightarrow x + y\sqrt{-5},\ x + y\sqrt{-5} \longrightarrow x - y\sqrt{-5}\}$. 2 and 5 are the only ramified primes since the discriminant is -20.

$\mathrm{Fr}_3(x+y\sqrt{-5}) \equiv (x+y\sqrt{-5})^3 \bmod (3, 1+\sqrt{-5})$, but $(x+y\sqrt{-5})^3 \equiv x^3 - 5\sqrt{-5}y^3 \equiv x+\sqrt{-5}y \pmod 3$, hence $\mathrm{Fr}_3(x+y\sqrt{-5}) \equiv (x+y\sqrt{-5})$ which is the identity automorphism.

$\mathrm{Fr}_{11}(x+y\sqrt{-5}) \equiv (x+y\sqrt{-5})^{11} \bmod (3, 1+\sqrt{-5})$, but $(x+y\sqrt{-5})^{11} \equiv x^{11} - 3125\sqrt{-5}y^{11} \equiv x-\sqrt{-5}y \pmod{11}$, hence $\mathrm{Fr}_{11}(x+y\sqrt{-5}) \equiv (x-y\sqrt{-5})$.

Here for an unramified prime integer p we have $\left(\frac{-5}{p}\right) = 1 \Longleftrightarrow \mathrm{Fr}_p$ is the identity automorphism $\Longleftrightarrow$ p splits completely in $\mathbb{Z}\left[\sqrt{-5}\right]$. By the Chinese remainder theorem and quadratic reciprocity $\left(\frac{-5}{p}\right) = 1 \Longleftrightarrow p \equiv 1, 3, 7, 9 \pmod{20}$.

$\mathrm{Ker(Ar)} = \{(a/b)\mathbb{Z} :\ b \neq 0,\ a, b$ are not divisible by 2 and 5, the number of prime divisors of a and b which are $\equiv 1, 3, 7, 9 \pmod{20}$ is even$\}$.

$\mathbb{Q}_{(2)\infty,1} = \{(1+20a/b)\mathbb{Z} :\ 1+20a/b$ is a positive integer, a and b are not divisible by 2 and 5$\}$ and $I_{(20)} = I_{(4)} = \{(a/b)\mathbb{Z} :\ a, b$ are not divisible by 2 and 5$\}$.

Here we have again $\mathbb{Q}_{(2)\infty,1} \subseteq \mathrm{Ker(Ar)} \subseteq I_{(4)}$ and $\mathrm{Sp}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q}) = \{p$ prime: $p \equiv 1$ or 3 or 7 or 9$\}$.

Example 4 $G\left(\mathbb{Q}(\zeta_m)/\mathbb{Q}\right) = \{\zeta_m \longrightarrow (\zeta_m)^k :\ k$ is a positive integer less than m and relatively prime to $m\}$, where ζ_m is a primitive m-th root of unity. It is known that the primes p which are not divisors of m are unramified and $\mathrm{Fr}_p(\alpha) = \alpha^p$ $\forall \alpha \in \mathbb{Q}(\zeta_m)$. If the order of the Frobenius automorphism is f, then the number of prime divisors of p in $\mathbb{Z}[\zeta_m]$ is $\phi(m)/f$, where f is the least positive integer such that $p^f \equiv 1 \pmod m$. Hence for the prime integer which is not a divisor of p we can say that $p \equiv 1 \pmod m \Longleftrightarrow \mathrm{Fr}_p$ is the identity automorphism $\Longleftrightarrow$ p splits completely in $\mathbb{Z}[\zeta_m]$.

In general, f is the least positive integer such that $p^f \equiv 1 \pmod m \Longleftrightarrow$ the order of Fr_p is f $\Longleftrightarrow$ the ideal generated by p in $\mathbb{Z}[\zeta_m]$ is a product of $\phi(m)/f$ distinct prime ideals.

$\mathrm{Ker(Ar)} = \{(a/b)\mathbb{Z} :\ b \neq 0;\ a, b$ are relatively prime to m and $a \equiv b \pmod m\}$.

$\mathbb{Q}_{(m)\infty,1} = \{(1+ma/b)\mathbb{Z} :\ 1+ma/b$ is a positive integer and a, b are relatively prime to $m\}$.

$I_{(m)} = \{(a/b)\mathbb{Z} :\ b \neq 0;\ a, b$ are relatively prime to $m\}$.

Here we also have $\mathbb{Q}_{(m)\infty,1} \subseteq \mathrm{Ker(Ar)} \subseteq I_{(m)}$ and $\mathrm{Sp}\left(\mathbb{Q}(\zeta_m)/\mathbb{Q}\right) = \{p$ prime: $p \equiv 1 \pmod m\}$.

6 The case of abelian field extension

As the generalization of these examples the Artin map is also onto for a finite abelian extension of $\mathbb{Q}$ and Ker(Ar) is contained in $\mathbb{Q}_{(m),1}$ or $\mathbb{Q}_{(m)\infty,1}$ for a positive integer m. This is the Artin Reciprocity Law as a generalization of quadratic and other reciprocity laws. $\mathrm{Ker(Ar)} = \mathbb{Q}_{(m),1} \cdot N_{\mathbb{K}/\mathbb{Q}}\left[I_{(m)}(\mathbb{K})\right]$ or $\mathrm{Ker(Ar)} = \mathbb{Q}_{(m)\infty,1} \cdot N_{\mathbb{K}/\mathbb{Q}}\left[I_{(m)}(\mathbb{K})\right]$. $N_{\mathbb{K}/\mathbb{Q}}\left[I_{(m)}(\mathbb{K})\right]$ is the image of the prime ideals which are relatively prime to the ideal in the ring of integers of $\mathbb{K}$ generated by m, under the norm map.

Conversely, there exists a finite abelian extension $\mathbb{K}$ of $\mathbb{Q}$ such that for a given positive integer $\left\{\begin{array}{c} m \\ m\infty \end{array}\right\}$ and a subgroup H such that $\left\{\begin{array}{c} \mathbb{Q}_{(m),1} \subseteq H \subseteq I_{(m)} \\ \mathbb{Q}_{(m)\infty,1} \subseteq H \subseteq I_{(m)} \end{array}\right\}$ and $H = \left\{\begin{array}{c} \mathbb{Q}_{(m),1} \cdot N_{\mathbb{K}/\mathbb{Q}}\left[I_{(m)}(\mathbb{K})\right] \\ \mathbb{Q}_{(m)\infty,1} \cdot N_{\mathbb{K}/\mathbb{Q}}\left[I_{(m)}(\mathbb{K})\right] \end{array}\right\}$. It is called the class field corresponding to the class group H.

We have also $\mathrm{Sp}(\mathbb{K}/\mathbb{Q}) \subseteq H$. We see also that the integers which can be written as x^2+y^2 are in Ker(Ar) which is between $\mathbb{Q}_{(4)\infty,1}$ and $I_{(4)}$ as we mentioned in the beginning of the article.

The results are true if we replace $\mathbb{Q}$ by a finite extension of $\mathbb{Q}$.

7 The case of nonabelian field extension

Unfortunately, it is not possible to characterize the set $\mathrm{Sp}(\mathbb{K}/\mathbb{Q})$ by the same method for a nonabelian finite Galois extension. As an example we take the Galois group of the polynomial $x^5 + 10x^3 - 10x^2 + 35x - 18$. The Galois group is not abelian. The only ramified primes are 2, 5, 11 since the discriminant $D = 2^6 5^8 11^2$. Here 7, 13, 19, 29, 43, 47 and 59 remain prime but 2063, 2213, 2953, 3631 split completely. What kind of pattern does there exist here if any?

The answer is given as some conjectures by the Langland's functoriality principle formulated in 1960 which includes a formulation of a nonabelian reciprocity law (local and global) as a special case. The global reciprocity law is formulated as a general conjectural correspondence between Galois representations and automorphic forms. Hecke character for the definition of Hecke L function is replaced by a cuspidal representation for a general automorphic L function. The global reciprocity law then is a statement relating Galois representations and cuspidal representations.

References

[1] Knapp A. W., *Introduction to Langlands Program*, Proceedings of Symposia in Pure Mathematics, Volume **61**, 1997, pp. 245–302.

[2] Janusz G. J., *Algebraic Number Fields*, 2nd ed., Graduate Studies in Mathematics, **7**, American Mathematical Society, Providence, RI, 1996.