Number Rings and Etale Coverings

Recall Fermat's theorem: an odd prime p is of the form $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$. We proved this using the point of view of finite field arithmetic and quadratic residues. Now we are going to shift our view once again (is this called capricious, flighty, mercurial, or fickle?) and see how it can do us a favor. Using the imaginary number $i = \sqrt{-1}$, we know that in this case p can be decomposed into the product $p = (x + yi)(x - yi)$, where

$$x \pm yi \in \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

are **Gaussian integers**.

Notice that the Gaussian integer ring $\mathbb{Z}[i]$, like $\mathbb{Z}$, is a **unique factorization domain** (UFD), i.e., every element in $\mathbb{Z}[i]$ can be uniquely decomposed into the product of prime elements. More precisely, if $a \in \mathbb{Z}[i]$ and there are two decompositions $a = \prod_{i=1}^{n} \alpha_i$ and $a = \prod_{j=1}^{m} \alpha_i'$, then $n = m$, and after a possible permutation, we have $(\alpha_i) = (\alpha_i')$, namely α_i and α_i' are the same up to a unit.

Now the above classical result of Fermat can be reformulated as the basic rule of prime decomposition in the bigger ring $\mathbb{Z}[i]$ (rather than the usual integer ring $\mathbb{Z}$) as follows.

Proposition 1. Let p be a prime number.

1. If $p \equiv 1 \pmod 4$, then $p = \alpha\bar{\alpha}$, where $\alpha, \bar{\alpha} \in \mathbb{Z}[i]$ are prime elements, $\bar{\alpha}$ is the conjugate of α and $(\alpha) \neq (\bar{\alpha})$.
2. If $p \equiv 3 \pmod 4$, then p is a prime element.
3. If $p = 2$, then $2 = (1 + i)^2 \times (-i)$, where $1 + i$ is a prime element and $-i$ is a unit.

Proof. 1. By Fermat's theorem, we can find integers $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$. Set $\alpha = x + yi$, then it suffices to show that $x + yi$ is a prime element. Define the **norm map**

$$\mathbb{N} : \mathbb{Z}[i] \to \mathbb{Z}_+, \quad a + bi \mapsto (a + bi)(a - bi) = a^2 + b^2,$$

then $\mathbb{N}$ is clearly multiplicative. Assume $x + yi = \alpha_1\alpha_2$, then taking norms gives $p = \mathbb{N}(x + yi) = \mathbb{N}(\alpha_1)\mathbb{N}(\alpha_2)$. Hence one of the $\mathbb{N}(\alpha_i)$'s is equal to 1, so it must be a unit and $x + yi$ is a prime element.

2. Suppose $p = \alpha_1\alpha_2$ is not a prime element, then taking norms gives that $\mathbb{N}(\alpha_1) = \mathbb{N}(\alpha_2) = p$. This contradicts that p is not of the form $x^2 + y^2$ by Fermat's theorem.

3. It follows from the fact that $\mathbb{N}(1 + i) = 2$ is a prime number.

□

Exercise. Show that $(\alpha) \neq (\bar{\alpha})$ in the first case to complete the proof.

So the arithmetic problem of the sum of two squares is essentially equivalent to finding the prime decomposition of p in the ring $\mathbb{Z}[i]$. This elegant point of view helps us to vastly and systematically generalize the arithmetic objects we study.

Definition 1. A **number field** K is a finite extension of the field $\mathbb{Q}$ of rational numbers. The elements of K are called **algebraic numbers**. The **number ring** (or **ring of integers**) $\mathcal{O}_K$ of K is the integral closure of $\mathbb{Z}$ in K. In concretely terms, $\mathcal{O}_K$ consists of **algebraic integers**, namely roots of monic polynomials in $\mathbb{Z}[x]$.

Example 1. The simplest number field other than $\mathbb{Q}$ is the $K = \mathbb{Q}(i)$, an imaginary quadratic extension of $\mathbb{Q}$. Let us compute the number ring of $K = \mathbb{Q}(i)$. Suppose $x = a+bi$ with $a, b \in \mathbb{Q}$. Then $x \in \mathcal{O}_K$ if and only if x satisfies a quadratic monic equation $X^2 - sX + t = 0$ with $s, t \in \mathbb{Z}$. We know that $2a = s$ and $a^2 + b^2 = t$. So $s^2 + 4b^2 = 4t$. Set $n = 2b$, then n is an integer and $s^2 + n^2 = 4t$. Therefore s and n are multiples of 2. We conclude that $a, b \in \mathbb{Z}$, so $\mathcal{O}_K = \mathbb{Z}[i]$, which is exactly the Gaussian integer ring.

Example 2. An important class of number fields are the **cyclotomic fields** $K = \mathbb{Q}(\zeta_n)$, generated by a primitive nth root of unity ζ_n. It has Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$. It can be shown in general that $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. In particular, taking $n = 4$ gives us again the Gaussian integer ring.

Exercise. Determine the ring of integers of the field $K = \mathbb{Q}(\sqrt{-7})$.

Remark. The cyclotomic fields were studied by Kummer in order to attack the Fermat's last theorem (Fermat, our old friend). Kummer factorized the equation $z^n = x^n + y^n$ as

$$z^n = (x + y)(x + \zeta_n y) \cdots (x + \zeta_n^{n-1} y).$$

To match the factors, he was forced to consider the prime decomposition in the ring $\mathbb{Z}[\zeta_n]$. However, a crucial caveat is that $\mathbb{Z}[\zeta_n]$ is not always a UFD, so the rule of unique decomposition into prime elements is not always possible.

Fortunately, Kummer considered a generalized notion of "ideals" and the decomposition of ideals into prime ideals is still available for all number rings. We state this version of the fundamental theorem of the arithmetic of number rings without proof.

Theorem 1. Let $\mathcal{O}_K$ be a number ring and $\mathfrak{a}$ be a nontrivial ideal of $\mathcal{O}_K$. Then $\mathfrak{a}$ can be uniquely (up to permutation) decomposed into a product of prime ideals

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_m^{e_m}, \quad e_i \geq 1.$$

Example 3. In $\mathbb{Z}[\sqrt{-5}]$. The element 6 has two decompositions $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ where none of $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ can be further decomposed. The problem occurring here is exactly that none of them generate prime ideals. The prime decomposition promised by the previous theorem is given by

$$(6) = (2, 1 + \sqrt{-5}) \cdot (2, 1 - \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5}).$$

As we have seen, in order to study the problem concerning rational numbers and integers, we need to work in a new world of extensions of $\mathbb{Q}$ and $\mathbb{Z}$, the number fields and number rings. It is amusing to compare this to the topological setting: in order to study the topology of a space, one way is to work with its unramified covering spaces instead. We now carry this key idea further, leading to the notion of **finite etale coverings** and **etale fundamental groups** in this algebraic setting.

space X	scheme $\operatorname{Spec} A$
unramified covering	finite etale covering
fundamental group	etale fundamental group

Let us look at several examples to motivate.

Example 4. One can define the fundamental group using loops. Though $\operatorname{Spec} A$ can be endowed with a topology (Zariski topology), but it is too coarse to contain any loop in the usual sense. Alternatively, we will define the etale fundamental group as the automorphism group of its "universal covering".

Example 5. However, another difference in the algebraic setting is that we cannot always expect the existence of the (usually **infinite**) universal covering. For example, the universal covering $\mathbb{R}^1 \to S^1$ is given by a transcendental function $t \mapsto e^{it}$, which does not make sense in the algebraic world. So we are going to step back and find an object which approximates all the **finite** etale coverings best.

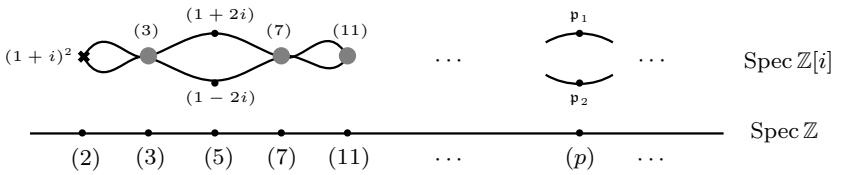
Example 6. Remember the ring $\mathbb{Z}$ corresponds to a space (an affine scheme) $\operatorname{Spec}\mathbb{Z}$, which can be geometrically represented by a line. A maximal ideal (p) corresponds to a closed point $\operatorname{Spec}\mathbb{F}_p \hookrightarrow \operatorname{Spec}\mathbb{Z}$. Unlike $\operatorname{Spec}\mathbb{C}[t]$, where all the residue fields are the same field $\mathbb{C}$, the points on $\operatorname{Spec}\mathbb{Z}$ have different residue fields $\mathbb{F}_p$, which are not algebraically closed. In other words, there are many finite extensions of $\mathbb{F}_p$ (one for each degree n). So we have many finite "covering spaces", although each of these covering spaces is also a point geometrically. Intuitively, we will draw a slightly bigger point to stand for those finite extensions $\operatorname{Spec}\mathbb{F}_{p^n}$. From this point of view, the space $\operatorname{Spec}\mathbb{F}_p$ is not "simply connected" because it has nontrivial finite covering spaces. It is now very natural to define the "fundamental group" of $\operatorname{Spec}\mathbb{F}_p$ as the automorphism group $\operatorname{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, viewing $\operatorname{Spec}\overline{\mathbb{F}_p}$ as the "universal covering" since $\mathbb{F}_p$ is the union of all finite extensions of $\mathbb{F}_p$.

Example 7. The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ gives a map $\pi : \operatorname{Spec}\mathbb{Z}[i] \to \operatorname{Spec}\mathbb{Z}$. The fiber of a prime $(p) \in \operatorname{Spec}\mathbb{Z}$ is given by $\operatorname{Spec}\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{F}_p = \operatorname{Spec}\mathbb{Z}[i]/(p\mathbb{Z}[i])$. From the prime decomposition in $\mathbb{Z}[i]$ we have the following situation:

(5)	$(1+2i)(1-2i)$	$\mathbb{Z}[i]/(5) \cong \mathbb{Z}[i]/(1+2i) \times \mathbb{Z}[i]/(1-2i) \cong \mathbb{F}_5 \times \mathbb{F}_5$	two points
(3)	(3)	$\mathbb{Z}[i]/(3) \cong \mathbb{F}_9$	one bigger point
(2)	$(1+i)^2$	$\mathbb{Z}[i]/(2) \cong \mathbb{F}_2[i] = \{0, 1, i, 1+i\}$	one double point

This matches the geometry:

1. For primes $p \equiv 1 \pmod 4$, $(p) = \mathfrak{p}_1\mathfrak{p}_2$. The $\mathfrak{p}_1$ and $\mathfrak{p}_2$ correspond to two points lying above $(p) \in \operatorname{Spec}\mathbb{Z}$.
2. For primes $p \equiv 3 \pmod 4$, $(p) = \mathfrak{p}$ remains prime, which corresponds to a slightly bigger point lying above $(p) \in \operatorname{Spec}\mathbb{Z}$.
3. For $p = 2$, $(2) = (1+i)^2$ is a power of prime, which corresponds to a double point geometrically. In this case the tensor product is no longer a field ($1+i$ is a nilpotent).



So only the last case the geometrical picture is not an unramified covering: two points are somehow collapsing together. This is characterized by the fact that $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{F}_p$ is not a field extension of $\mathbb{F}_p$.

With the above said, it is not at all absurd to introduce the following definition, with the mind that "etale" is intended to mean an unramified covering in the algebraic setting.

Definition 2. Let k be a field. An k-algebra is called **finite etale** if it is a finite product of finite separable extension of k.

Definition 3. A map $\operatorname{Spec} B \to \operatorname{Spec} A$ (or equivalently, a ring homomorphism $A \to B$) is called a **finite etale** map if B is a finitely generated flat A-module and for any prime $\mathfrak{p} \in \operatorname{Spec} A$, $B \otimes_A \kappa(\mathfrak{p})$ is a finite etale $\kappa(\mathfrak{p})$-algebra, where $\kappa(\mathfrak{p}) = \operatorname{Frac}(A/\mathfrak{p})$ is the residue field of $\mathfrak{p}$. In this case we say that B is a **finite etale A-algebra** or $\operatorname{Spec} B$ is a **finite etale covering** of $\operatorname{Spec} A$.

Next time we will define the etale fundamental group in terms of finite etale coverings and make more concrete sense with examples.