More etale fundamental groups

Last time we computed the etale fundamental group of $\operatorname{Spec}\mathbb{F}_p$ to be $\operatorname{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}}$. The same arugment goes for the etale fundamental group of the spectrum of any field.

Example 1. In general, for a field F, the etale fundamental group of $\operatorname{Spec} F$ is the **absolute Galois group** $\operatorname{Gal}(F^s/F)$, where F^s is the separable closure of F (by the same argument). The absolute Galois group of $\mathbb{Q}$ contains monstrous secrets about all number fields and thus is of great interest to study in number theory. People are far from understanding the whole absolute Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as of today.

Our next goal is to compute the etale fundamental group $\pi_1(\operatorname{Spec}\mathbb{Z})$. The following algebraic fact allows us to consider only the etale coverings arising from number rings.

Theorem 1. Suppose $\operatorname{Spec} A$ is normal (i.e., A is an integrally closed domain). Let K_i be a finite extension of $\operatorname{Frac}(A)$ and B_i be the integral closure of A in K_i. Then the universal covering is $\tilde{X} = \varprojlim_i X_i$, where X_i runs over the $\operatorname{Spec} B_i$ such that $\operatorname{Spec} B_i \to \operatorname{Spec} A$ is finite etale.

Remark. Indeed, the same thing is true for an arbitrary normal scheme.

Now applying the theorem to the normal ring $A = \mathbb{Z}$, to determine $\pi_1(\operatorname{Spec}\mathbb{Z})$ it suffices to find all the number rings $\mathcal{O}_K$ that are finite etale over $\mathbb{Z}$. From the point of view of prime decomposition, this means in the decomposition of each prime

$$(p) = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}$$

in $\mathcal{O}_K$, all the e_i's are equal to 1.

Definition 1. A prime $p \in \mathbb{Z}$ is called **unramified** in $\mathcal{O}_K$ if all the e_i's are equal to 1, and **ramified** otherwise. The e_i is called the **ramification index** of $\mathfrak{p}_i$.

So the K_i's in the previous theorem are exactly the number fields unramified at each p. If we define the **maximal unramified extension** $\mathbb{Q}^{ur}$ of $\mathbb{Q}$ as the union of all such $K_i's$, then $\pi_1(\operatorname{Spec}\mathbb{Z}) = \operatorname{Gal}(\mathbb{Q}^{ur}/\mathbb{Q})$. To compute $\mathbb{Q}^{ur}$, the key input is to relate the ramification behavior of primes to the numerical invariant of number rings — the discriminant.

Definition 2. Let K be a number field of degree n and $\{\alpha_j\}_{j=1}^n$ be a $\mathbb{Z}$-basis of the number ring $\mathcal{O}_K$. Then we define the (absolute) **discriminant** $d_K = (\det(\sigma_i(\alpha_j))_{ij})^2$, where σ_i runs over the embeddings $K \hookrightarrow \mathbb{C}$. The discriminant is an integer independent of the choice of the $\mathbb{Z}$-basis.

We omit the proof of the following important theorem.

Theorem 2. A prime p is ramified in $\mathcal{O}_K$ if and only if $p \mid d_K$.

Example 2. Let $K = \mathbb{Q}(i)$. We know that $\{1, i\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[i]$. So

$$d_K = \left(\det\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}\right)^2 = (-2i)^2 = -4.$$

The previous theorem tells us that only the prime 2 is ramified in $\mathbb{Z}[i]$, which coincides with what we discovered before.

Exercise. Let p be an odd prime. Determine which primes are ramified in the cyclotomic field $K = \mathbb{Q}(\zeta_p)$.

So showing that a number field K is unramified everywhere is equivalent to showing that $|d_K| = 1$. Are there any such number fields? Minkowski used his method of geometry of numbers to bound $|d_k|$ from below.

Theorem 3 (Minkowski)**.** *Let K be a number field of degree n . Then*

$$|d_K|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}.$$

Corollary 1. *If K is a number field other than $\mathbb{Q}$, then $|d_K| > 1$.*

Proof. Minkowski's theorem gives that $|d_K| \geq a_n := \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^n$. The result then follows since $a_2 = \pi^2/4 > 1$ and $a_{n+1} \geq a_n$. □

Combining Theorem 2 with the previous corollary, we know that the only number ring unramified everywhere over $\mathbb{Z}$ is $\mathbb{Z}$ itself (thus there is no nontrivial finite etale $\mathbb{Z}$-algebra except $\mathbb{Z}^n$). So the maximal unramified extension $\mathbb{Q}^{ur} = \mathbb{Q}$ and we have

Corollary 2. $\pi_1(\operatorname{Spec}\mathbb{Z}) = 1$.

We collect our computation so far as follows. If my (or Charmaine's) word that $\operatorname{Spec}\mathbb{Z}$ is "3-dimensional" can be trusted, then it is natural to believe that $\operatorname{Spec}\mathbb{Z}$ should behave like a "simply connected 3-manifold".

$K : S^1 \hookrightarrow \mathbb{R}^3$	$\operatorname{Spec}\mathbb{F}_p \hookrightarrow \operatorname{Spec}\mathbb{Z}$
$\pi_1(S^1) = \mathbb{Z}$	$\pi_1(\operatorname{Spec}\mathbb{F}_p) = \hat{\mathbb{Z}}$
$\pi_1(\mathbb{R}^3) = 1$	$\pi_1(\operatorname{Spec}\mathbb{Z}) = 1$

We can easily add a new row concerning the knot group $G_K = \pi_1(\mathbb{R}^3 \setminus K)$. The knot group corresponds to the unramified coverings of $\mathbb{R}^3 \setminus K$, so the arithmetic counterpart should correspond to the finite etale coverings of $\operatorname{Spec}\mathbb{Z} \setminus \{p\}$, or equivalently $\operatorname{Spec}\mathbb{Z}[1/p]$ (we can kill the prime ideal (p) by inverting p).

Definition 3. We define the **prime group** to be the etale fundamental group

$$G_{\{p\}} := \pi_1(\operatorname{Spec}\mathbb{Z} \setminus \{p\}) = \pi_1(\operatorname{Spec}\mathbb{Z}[1/p]).$$

Even though there are no nontrivial finite etale coverings of the whole space $\operatorname{Spec}\mathbb{Z}$, there do exist finite coverings of $\operatorname{Spec}\mathbb{Z}$ that are etale outside a prime p (e.g., our favorite example $\operatorname{Spec}\mathbb{Z}[i] \to \operatorname{Spec}\mathbb{Z}$ is etale outside 2), so the prime group may be nontrivial.

What is the right analogy for the tubular neighborhood V_K of a knot K? This is not that easily seen and leads to the beautiful idea of completion. It is already quite surprising that we have gone so far away without even mentioning p-adic numbers.

Example 3. Consider the complex line $\mathbb{A}^1 = \operatorname{Spec}\mathbb{C}[t]$. The point $\{0\} \hookrightarrow \mathbb{A}^1$ corresponds to the quotient map $\mathbb{C}[t] \to \mathbb{C}[t]/(t) \cong \mathbb{C}$. How do we describe a neighborhood of $\{0\}$ algebraically? Notice that $\mathbb{C}[t] \to \mathbb{C}[t]/(t)$ is nothing but the evaluation map $f \mapsto f(0)$, which only gives the information about the point $\{0\}$. If we would like to remember the first derivative of f, then the quotient map $\mathbb{C}[t] \to \mathbb{C}[t]/(t^2)$ is better. Geometrically, the nilpotent element t adds a bit of "fuzz" to the point along the t direction (we have seen a similar example

$\mathbb{Z}[i]/(1+i)^2$ before), so $\operatorname{Spec}\mathbb{C}[t]$ stands for a double point (as the intersection of a parabola $y=t^2$ and the line $y=0$). In general, the quotient map $\mathbb{C}[t]\to\mathbb{C}[t]/(t^{n+1})$ remembers all derivatives of f up to order n and provides us an order n "fuzz" around the point. Of course there is no reason to stop us at any specific n. So we can take the inverse limit of the inverse system

$$\cdots\to\mathbb{C}[t]/(t^n)\to\mathbb{C}[t]/(t^{n-1})\to\cdots\to\mathbb{C}[t]/(t),$$

which is exactly the power series ring

$$\varprojlim_n \mathbb{C}[t]/(t^n)=\mathbb{C}[[t]].$$

We call $\mathbb{C}[[t]]$ the **completion** of $\mathbb{C}[t]$ at the prime ideal (t). It provides geometrically an infinitesimal neighborhood of the point $t=0$ to help us read the local information about that point.

Example 4. We now mimic the completion process of $\mathbb{C}[t]$ at $t=0$ to give an infinitesimal neighborhood of $\operatorname{Spec}\mathbb{F}_p\hookrightarrow\operatorname{Spec}\mathbb{Z}$. We take the inverse limit of the inverse system

$$\cdots\to\mathbb{Z}/(p^n)\to\mathbb{Z}/(p^{n-1})\to\cdots\to\mathbb{Z}/(p),$$

and define

$$\mathbb{Z}_p:=\varprojlim_n \mathbb{Z}/(p^n).$$

As a group, $\mathbb{Z}_p$ is profinite. Even more, since each of the finite group $\mathbb{Z}/(p^n)$ is of p-power order, $\mathbb{Z}_p$ is a **pro-p group** and it is the **pro-p completion** of $\mathbb{Z}$. Geometrically, $\operatorname{Spec}\mathbb{Z}_p$ should be thought of as an infinitesimal neighborhood of $\operatorname{Spec}\mathbb{F}_p$ encoding all the local information of $\operatorname{Spec}\mathbb{Z}$ at p.

$K:S^1\hookrightarrow\mathbb{R}^3$	$\operatorname{Spec}\mathbb{F}_p\hookrightarrow\operatorname{Spec}\mathbb{Z}$
$\pi_1(S^1)=\mathbb{Z}$	$\pi_1(\operatorname{Spec}\mathbb{F}_p)=\hat{\mathbb{Z}}$
$\pi_1(\mathbb{R}^3)=1$	$\pi_1(\operatorname{Spec}\mathbb{Z})=1$
$G_K=\pi_1(\mathbb{R}^3\setminus K)$	$G_{\{p\}}=\pi_1(\operatorname{Spec}\mathbb{Z}[1/p])$
V_K	$\operatorname{Spec}\mathbb{Z}_p$

Definition 4. The elements of the ring $\mathbb{Z}_p$ are called **p-adic integers**.

We do not know much about the p-adic integers but the following exercise can be tackled right now.

Exercise. Show that $\hat{\mathbb{Z}}\cong\prod_p\mathbb{Z}_p$, where p runs over all primes numbers.

In the sequel we will investigate more basic properties of $\mathbb{Z}_p$, study the prime group $G_{\{p\}}$ using class field theory, and reinterpret the Legendre symbol to draw the connection to linking numbers at last.