

## 2. LECTURE 2. Betti cohomology, etale cohomology and $l$ -adic cohomology.

**2.1. Etale cohomology.** Let  $X$  be an algebraic variety over an algebraically closed field  $L$ . In 1940-th A. Weil conjectured that in some cases one can define **in purely algebraic terms** the cohomology groups  $H^*(X, A)$  that have good functorial properties and in case when  $L = \mathbb{C}$  would coincide with the groups  $H^*(X_{an}, A)$ .

This program has been realized by A. Grothendieck. Namely, given a finite abelian group  $A$  such that the size  $\#(A)$  is prime to the  $p = \text{char}(L)$  he defined the etale cohomology groups  $H_{et}(X, A)$  that have all the desired properties.

**2.2.  $l$ -adic cohomology.** Using this construction Grothendieck defined a family of cohomology theories for such varieties. Namely, for every prime number  $l$  prime to  $\text{char}(L)$  he defined  $l$ -adic cohomology functors

$$\begin{aligned} H^*(X, \mathbb{Z}_l) &:= \varprojlim H^*(X, \mathbb{Z}/l^k\mathbb{Z}) \\ H^*(X, \mathbb{Q}_l) &:= \mathbb{Q}_l \otimes_{\mathbb{Z}_l} H^*(X, \mathbb{Z}_l) \\ H^*(X, \bar{\mathbb{Q}}_l) &:= \bar{\mathbb{Q}}_l \otimes_{\mathbb{Q}_l} H^*(X, \mathbb{Q}_l). \end{aligned}$$

In fact Grothendieck and his group has done much more.

Constructible sheaves, Six functors etc.

**2.3. Cohomology of elliptic curves.** I will use these cohomology theories and their properties without proofs. But in order to show what are the difficulties and limitations of these theories I will consider a special case where all these theories could be described much more explicitly.

*Example 2.3.1.* Consider an elliptic curve  $E$  over an algebraically closed field  $L$ . The set  $E(L)$  of  $L$ -points of  $E$  has a natural structure of an abelian group.

For every natural number  $n$  consider the multiplication morphism  $[n] : E \rightarrow E$ . This morphism is epimorphic, and we denote by  $E(n) \subset E(L)$  the kernel of this morphism.

**2.3.2.** Consider the case when  $L = \mathbb{C}$ . In this case we have an analytic realization  $E_{an}$  of our curve as  $E_{an} = \mathbb{C}/\Lambda$ , where  $\Lambda$  is some lattice in  $\mathbb{C}$ . From this realization can easily describe all topological invariants of the space  $E_{an}$ .

**Claim.** (i)  $H_1(E_{an}, \mathbb{Z}) = \Lambda$ ,  $H^1(E_{an}, \mathbb{Z}) = \Lambda^*$

(ii)  $E(\infty) = \mathbb{Q}/\mathbb{Z} \otimes \Lambda$  and for every  $n$  we have  $E(n) = \frac{1}{n}\Lambda/\Lambda \approx (\mathbb{Z}/n\mathbb{Z})^2$

All information about the lattice  $\Lambda$  that we can extract from the algebraic curve  $E$  is encoded into the group  $E(\infty)$ . It allows to reconstruct many objects related to the group  $\Lambda = H_1(E_{an}, \mathbb{Z})$ , but not  $\Lambda$  itself. Here are some of constructions.

(i) Let  $l$  be a prime number. Consider the  $\mathbb{Z}_l$ -module  $T_l(E) := \text{Mor}(\mathbb{Q}_l/\mathbb{Z}_l, E(\infty))$ . Then it is equal to the  $l$ -adic completion of the lattice  $\Lambda$ , i.e. to the  $\mathbb{Z}_l$ -module  $\mathbb{Z}_l \otimes \Lambda$ .

(ii) The  $\mathbb{Q}_l$ -module  $T'_l = \mathbb{Q}_l \otimes_{\mathbb{Z}} \Lambda$  can be described as the group of continuous morphisms

$\text{Mor}_{con}(\mathbb{Q}_l, E(L)) = \text{Mor}_{con}(\mathbb{Q}_l, E(\infty))$ , where  $E(L)$  is considered with discrete topology.

**2.3.3.** From Lefschetz principle we can see that we can prove similar results for any algebraically closed field  $L$  of characteristic 0. Namely, we claim that

- (i)  $E(n) \approx (\mathbb{Z}/n\mathbb{Z})^2$
- (ii) The  $\mathbb{Z}_l$  module  $T_l(E) : Mor(\mathbb{Q}_l/\mathbb{Z}_l, E(L))$  is isomorphic to  $\mathbb{Z}_l^2$
- (iii) The module  $T'_l(E) = Mor_{con}(\mathbb{Q}_l, E(L))$  is isomorphic to  $\mathbb{Q}_l^2$ .

In case when  $L$  is an algebraically closed field of characteristic  $p > 0$  the same results hold provided  $n$  and  $l$  are prime to  $p$ . They are not correct if this does not hold.

This explains what are limitations of these cohomology theories and why they behave badly if  $l$  equals to the characteristic of  $L$ .

**2.4. Action of Galois groups.** Main advantage of the theories defined by purely algebraic constructions is that they produce representations of Galois groups. Namely, suppose we are given a field  $K$ . Fix an algebraic closure  $L = \bar{K}$  and denote by  $\Gamma$  the Galois group  $\Gamma = \text{Gal}(L/K) = \text{Aut}_K(L)$ .

Suppose we are given an algebraic variety  $Y$  defined over  $K$ . Let us denote by  $X = Y_L$  the variety over  $L$  obtained from  $Y$  by extension of scalars. Then the Galois group  $\Gamma$  acts on the scheme (variety)  $X$  and this induces the action of  $\Gamma$  on all cohomology spaces associated to  $X$  —  $H_{et}(X, A)$ ,  $H(X, \mathbb{Z}_l)$ ,  $H(X, \mathbb{Q}_l)$ . Thus, starting from the variety  $Y$  we produce families of representations of the group  $\Gamma$ . We usually will denote these representations by  $\rho$  or  $\rho_l$ .

*Remarks.* 1. This construction gives a way to construct interesting families of Galois representations. In fact, this gives a powerful tool to study Galois groups – they are some of the most important characters in Number Theory.

2. Starting with the variety  $Y$  we constructed the whole series of representations  $(\rho_l, \Gamma, H^i(X, \mathbb{Q}_l))$ . If you look at their construction, even in the simple case when  $Y$  is an elliptic curve defined over  $K$ , you do not see any direct relations between these representations.

On the other hand one feels that in some sense this is the same representation – in slightly different disguises. One can suspect that in fact there exists some representation  $\rho$  in vector space over  $\mathbb{Q}$  that produces these representations (at least for almost primes  $l$ ).

This suggestion is probably not correct as stated. However, I personally think that there exists some “small” object  $\rho$  that allows to reconstruct these representations  $\rho_l$  for almost all  $l$ .

**2.4.1. Case of  $p$ -adic fields.** Let  $K$  be a number field. Consider its non-Archimedean valuation  $\mathfrak{p}$  and denote by  $K_{\mathfrak{p}}$  the completion of  $K$  with respect to this valuation.

Here we can think about the case when  $K = \mathbb{Q}$ ,  $K_{\mathfrak{p}} = \mathbb{Q}_p$ .

It is known that the absolute Galois group  $\Gamma_{\mathfrak{p}}$  can be naturally embedded into  $\Gamma$  (this

Let as before  $L = \bar{K}$  and  $\Gamma = \text{Gal}(L/K)$ ). Consider the family of representations  $\rho_l$  of the type describe above.

In order to study a representation  $\rho$  of the global Galois group  $\Gamma$  it is usually useful to first study its restriction to a local Galois group  $\Gamma_{\mathfrak{p}}$ . So, let us consider a representation  $\rho_l$  restricted to the local Galois subgroup  $\Gamma_{\mathfrak{p}}$ .

We will see that in case when  $l$  is not equal to the residual characteristic  $p$  of the field  $K_{\mathfrak{p}}$  the structure of any continuous representation of the Galois group  $\Gamma_{\mathfrak{p}}$  is relatively simple. Thus the most difficult and interesting case is when  $l = p$ . This is exactly the subject of the  $p$ -adic Hodge theory.



**2.5. Structure of the local Galois group and its representations.** In this course we will mostly deal with local Galois groups.

Let us fix a  $p$ -adic field  $K$  that is a finite extension of the field  $\mathbb{Q}_p$ . We fix a discrete valuation  $v : K \rightarrow \mathbb{Q} \cup \{\infty\}$  normalized by condition  $v(p) = 1$ . We denote by  $O = O_K$  the ring of integers,  $O_K = \{x \in K | v(x) \geq 0\}$ . Let  $\mathfrak{p} = \mathfrak{p}_+ K := \{x \in O_K | v(x) > 0\}$  be the maximal ideal of  $K$  and  $k = O_K/\mathfrak{p}$  the finite residue field.

Fix the algebraic closure  $L/K$  and denote by  $G$  the Galois group  $Gal(L/K)$ . We extend the valuation  $v$  to the field  $L$  (this is not a discrete valuation). Using the valuation  $v$  we define the ring of integers  $O_L \subset L$  – this is the integral closure of the ring  $O_K$  in  $L$ .

The ring  $O_L$  is a local ring and the residue quotient field  $l = O_L/\mathfrak{p}_L$  is an algebraic closure of the residue field  $k$ .

From this construction we see that there is a canonical morphism  $p : Gal(L/K) \rightarrow Gal(l/k)$ . It is known that this morphism is epimorphic.

The group  $Gal(l/k)$  is isomorphic to the group  $\hat{\mathbb{Z}}$ . In fact this isomorphism is canonical since this group has the distinguished element – Frobenius morphism –  $FR = Fr_q$ , where  $q := \#(k)$ . This element plays a central role in the theory.

The kernel of the morphism  $p : \text{Gal}(L/K) \rightarrow \text{Gal}(l/k)$  is called the **inertia group** of  $K$ . We denote this subgroup by  $I_K$ .

**Definition.** A representation  $\rho$  of the group  $\text{Gal}(L/K)$  is called **unramified** if it is trivial on the inertia subgroup  $I_K$ .

An unramified representation  $(\rho, V)$  can be considered as a representation of the quotient group  $\text{Gal}(l/k)$ . In particular it defines an automorphism  $Fr : V \rightarrow V$  equal to  $\rho(Fr_q)$ .

Let  $Y$  be a smooth projective variety defined over the field  $K$ . We say that  $Y$  has a **good reduction** if it can be realized over the ring  $O_K$  in such a way that the quotient variety  $\bar{Y}$  over the field  $k$  is again smooth and projective.

**Theorem 2.6.** *Suppose that a variety  $Y$  over the field  $K$  has good reduction. Fix a prime number  $l$  different from the characteristic  $p$  of the field  $k$ .*

*Then the representation  $(\rho_l, \text{Gal}(L/K), H^*(X, \mathbb{Q}_l))$  of the group  $\text{Gal}(L/K)$  is unramified.*

*Moreover, there exists a canonical isomorphism of vector spaces  $H^*(X, \mathbb{Q}_l)$  and  $H^*(\bar{X}, \mathbb{Q}_l)$  compatible with the action of the Galois group  $\text{Gal}(L/K)$ .*

In case when  $Y = E$  is an elliptic curve this follows from the statement the the reduction map  $E(n) \rightarrow \bar{E}(n)$  is bijective for any  $n$  prime to  $p$ .

$$\text{char } k = p$$

$\Gamma = \text{Gal}(L/k)$  acts on  $p$ -adic space

$$H^i(X, \mathbb{Q}_p).$$

Structure of  $\Gamma = \text{Gal}(L/k)$   
 $k$ - $p$ -adic field.

$$\text{Gal}(L/k)$$

$$1 \rightarrow I_k \rightarrow \text{Gal}(L/k) \rightarrow \bar{G} \rightarrow 1$$

Group  $I_k$  corresponds to the maximal unramified field extension  $k^{\text{un}} \subset L$

$$I_k = \text{Gal}(L/k^{\text{un}}).$$

$$k^{\text{un}} = k(\sqrt[n]{a}), \text{ for all } n \text{ prime to } p.$$

$$k^{\text{tr}} = k^{\text{un}}(\sqrt[n]{a} \mid n \text{ prime to } p)$$

$$\frac{(k^{\text{un}})^*}{(k^{\text{un}})^*} = \mathbb{F}_p$$

corresponding s.s. of  $\Gamma$   
is denoted  $W_e$ -where  
verification group.

Lemma  $I_K/W_K \cong \sum_{e \neq p}^{\neq p} \cong \prod_{e \neq p} \mathbb{Z}_e$

clearly  $W_p$  is a  $p$ -group.

structure of  $\Gamma = \text{Gal}(L/K)$

$$\Gamma \supset I_K \supset W_K \text{ normal s.s.}$$

$$\Gamma/I_K \cong \sum^1, \text{ generated by } v$$

$$I_K/W_K \cong \sum^{\neq p}$$

$W$  is a  $p$ -group.

corollary. let  $e \neq p$  then  
for any continuous rep.

$\rho: \Gamma \rightarrow \text{End}(V)$  if some  
from  $e$ -adic vector space.  
we have  $|\rho(W_K)|$  is finite.

$$\rho: \Gamma \rightarrow \text{GL}(V)$$

$$\rho|_{W_K}$$

If  $\bar{e} = p$  then  $p$ -adic reps  
 of  $\Gamma$  are quite non-trivial  
 since they are quite  
 non-trivial on  $U_K$ .

---

Cyclotomic character.

$$N = K(\sqrt[p^k]{1}) \subseteq L = \bar{K}$$

$\Gamma$  acts on  $N$ , i.e. acts on  
 the  $p^k$ -th roots of unity  
 $\sqrt[p^k]{1}$

$$R = (\mathbb{Q}_p / \mathbb{Z}_p) =$$

$$R = \mathbb{G}_m[p^\infty] \subset L^*$$

$\Gamma$  acts on  $R$ .

$$\begin{aligned} T(R) &= \text{Hom}(\mathbb{Q}_p / \mathbb{Z}_p, L^*) = \\ &= \text{Hom}(\mathbb{Q}_p / \mathbb{Z}_p, R) \end{aligned}$$

$$\Gamma \text{ acts on } T(R), \quad T(R) \cong \mathbb{Z}_p$$

1-dim.  $\mathbb{Z}_p$ -rep of  $\Gamma$  over  $\mathbb{Z}_p$   
 Given by  $\rho(\gamma) = X(\gamma)$

$$\rho(\gamma)(x) = x^{X(\gamma)} \quad x \in \mathbb{Z}_p$$

$x \in \mathbb{P}$ ,  $a \in \mathbb{Z}_p$  then  
we can define  $x^a$ .