NOTES ON TALK 1. ANABELIAN GEOMETRY: INTRODUCTION

ALENA PIRUTKA

1. What is contained in "Galois type" data?

Gauss: The regular n-gon can be constructed by straightedge and compass if and only if $n = 2^k p_1 \dots p_r$ where $p_i = 2^{2^{n_i}} + 1$ are Fermat primes. For example, $n = 17$. (Based on the study of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ and cyclotomic polynomials). Here the key is that the hidden symmetries are in the Galois group action (not in the geometric symmetry). Later we will consider the "hidden" structures in the absolute Galois group of a field (such as a projective structure).

1.1. **Inverse Galois Problem.**

- *Inverse Galois Problem:* which finite groups G can be realized as Galois groups of an extension over $\mathbb{Q}$? (OPEN).
  Hilbert: yes for groups G that can be realized as a Galois group of $K = \mathbb{Q}(x_1, \dots x_r)$.
  Noether: If V is a (linear) representation of a finite group G over the field k, then $G = Gal(k(V) : k(V)^G)$ so that if $k(V)^G$ is purely transcendental over k and $k = \mathbb{Q}$, one can apply Hilbert's theorem: G is a Galois group over $\mathbb{Q}$.
- Remark: Shafarevich showed that any solvable finite group is a Galois group over $\mathbb{Q}$.

1.2. **Noether Problem.**

When $k(V)^G/k$ is purely transcendental? I.e. when V/G is rational?

Counterexamples (when $k(V)^G/k$ is not purely transcendental) with k algebraically closed:

- Saltman (1984): G of order ℓ^9;
- Bogomolov (1988): G of order ℓ^6;
- Moravec (2011): G of order ℓ^5;
- more examples for nonlinear actions.

Counterexamples with $k = \mathbb{Q}$:

- Swan, Voskresenskii: $G = \mathbb{Z}/47$;
- Saltman, Voskresenskii: $G = \mathbb{Z}/8$.

Date: January 6, 2018.

In section 2 we discuss in details the examples of F. Bogomolov: the invariants that obstruct the rationality of V/G come from (a quotient of) the absolute Galois group of $k(V)^G$: more precisely, from the subgroup of unramified elements in the second Galois cohomology of this group.

1.3. **Reconstructing of fields from their absolute Galois group.** The discussion above motivates the following question: how much one can read from the absolute Galois group $G_k = Gal(k^{sep}/k)$ of a field k? Could one "reconstruct" the field from its Galois-theoretic invariant(s)?

- Artin-Schreier (1920): if G_k is a finite non-trivial group, then $G_k \simeq G_{\mathbb{R}} = \mathbb{Z}/2$ and k is real closed. Here $G_{\mathbb{R}}$ is simple to understand.
- The group $G_{\mathbb{Q}_p}$ (more generally, G_k for k a p-adic field), $p \neq 2$, is much more complicated, but its structure is known (Jakovlev, Poitou, Jannsen-Wingberg and others), see Neukirch, Schmidt, *Cohomology of Number Fields*, section 7.5. The Galois group $\mathcal{G}_k$ of the maximal tamely ramified extension is a profininte group generated by two elements σ, τ with one relation $\sigma\tau\sigma^{-1} = \tau^q$ (where q is the cardinality of the residue field). The wild ramifiation group is a pro-p-subgroup and is also described by generators and relations (cf. the explicit desciption by Demuskin). Jannsen-Wingberg give the complete description: if $[k : \mathbb{Q}_p] = n$, then G_k is a profinite group with $n+3$ generators $\sigma, \tau, x_0, \dots x_n$, satisfying the explicit relations (too long to copy it here).
- Neukirch (1969, a p-adic analogue of Artin-Schreier result): if $k \subset \bar{\mathbb{Q}}$ and $G_k \simeq G_{\mathbb{Q}_p}$, then k is the decomposition field of an extension of $| \, |_p$ to $\bar{\mathbb{Q}}$ (extended by Pop to the general case, not necessarily a subfield of $\bar{\mathbb{Q}}$).
- Example of Perlis: non-isomorphic field extensions of $\mathbb{Q}$, with the same Dedekind zeta-functions (i.e. this local data does not determine the field).
- Uchida (1976) (notes by Iwasawa, unpublished): the Galois group characterizes a global field. More precisely, if k, k' are global fields with

  $G_k \overset{\phi}{\simeq} G_{k'}$ as profinite groups, then $k \simeq k'$ as fields: there exits a field isomorphism $\psi : {k'}^{sep} \to k^{sep}$ with $\psi(k') = k$ and $\phi(g) = \psi^{-1} \circ g \circ \psi$.

  Remark: it is enough to have an isomorphism between Galois groups of maximal solvable extensions of k and k'.
- Pop: generalization to arbitrary fields. There is a "group-theoretical recipe" to recover finitely generated infinite fields k from their absolute Galois groups G_k. Moreover, the same fonctoriality property as above holds. (Also, there are results by Mochizuki for the correspondance between homomorphisms $G_k \to G_{k'}$ and embeddings of fields $k \to k'$). Some steps in the argument:
  a) view k as a function field of a normal complete scheme over $\mathbb{Z}$ or over $\mathbb{F}_p$;
  b) develop an analogue of the Neukirch's local theory: in higher dimensions, places correspond to valuations, whose decomposition and inertia groups are encoded in G_k;
  c) recover k from the local data (a difficulty is to indentify k in $\hat{k}$).
- Bogomolov's anabelian program, results by Bogomolov-Tschinkel: the entire group G_k is too large and often difficult to understand. The goal is to

reconstruct the field k from much smaller amount of data. Let $\mathcal{G}_k$ be a pro-ℓ-completion of G_k for $\ell \neq char\, k$. Let $\mathcal{G}_k^a$ be the abelinization $\mathcal{G}_k^a = \mathcal{G}_k/[\mathcal{G}_k, \mathcal{G}_k]$ and $\mathcal{G}_k^c = \mathcal{G}_k/[\mathcal{G}_k, [\mathcal{G}_k, \mathcal{G}_k]]$ the canonical central extension. Let Σ_k be the set of all (topologically) non-cyclic subgroups of $\mathcal{G}_k^a$ that lift to abelian subgroups of $\mathcal{G}_k^c$. The main result (see also Pop, *On the birational anabelian program initiated by Bogomolov I*) says that if k is a function field of an algebraic variety over $\bar{\mathbb{F}}_p$, then the couple $(\mathcal{G}_k^a, \Sigma_k)$ determines k. Should also work (to do!) over *any* algebraically closed field (not only over $\bar{\mathbb{F}}_p$).

1.4. **Curves and the fundamental group.** To a connected scheme X with a geometric base point $\bar{x}$ one associates the étale fundamental group $\pi_1(X, \bar{x})$, defined as the automorphism group of the fiber functor on the category of the étale covers of X. We will ignore the point $\bar{x}$ and write simply $\pi_1(X)$ (more accurately, we view $\pi_1(X)$ in the category of all profinite groups with outer continuous homomorphisms). If X is a geometrically connected scheme over a field k, then there is an exact sequence:

$$1 \to \pi_1(\bar{X}) \to \pi_1(X) \to G_k \to 1.$$

If $k \subset \mathbb{C}$, then, the base change to $\mathbb{C}$ realizes $\pi_1(\bar{X})$ as the profinite completion of the topological fundamental group of $X(\mathbb{C})$.

If X is complete and regular, $\pi_1(X)$ is a birational invariant.

Now assume that X is a smooth and connected curve, X^c is a smooth compactification, $S = X^c \setminus X$, $g = g(X^c)$ and $r = |\bar{S}|$. Recall that X is hyperbolic if $2-2g-r < 0$. If $char k = 0$, then the group $\pi_1(\bar{X})$ is well understood via generators and relations ($2g$ generators and one relation for X complete, and free with $2g+r-1$ for $r > 0$ and X not isomorphic to $\mathbb{A}^1$). In positive characteristic, one considers the *tame fundamental group* $\pi_1^t(X)$ as the maximal quotient of $\pi_1(X)$ that classifies étale connected covers $X' \to X$ whose ramification is tame above the points in S.

Following Grothendieck, a property of X is *anabelian* if it is encoded in the fundamental group $\pi_1(X)$:

- Anabelian conjecture for curves: an isomorphism type of X can be recovered from $\pi_1(X)$ (up to pure inseparable covers and Frobenious twists), functorially with respect to isomorphisms and homomorphisms, as in Uchida's and Mochizuki's results. I.e. do we have $Hom_k(X,Y) = Hom_{G_k}(\pi_1(X), \pi_1(Y))/\sim$? (note: by Faltings, for X, Y abelian varieties over a number field, we have $Hom_{G_k}(\pi_1^a(X), \pi_1^a(Y)) = Hom_k(X,Y) \otimes \hat{\mathbb{Z}}$.)
- Section conjecture (resp. birational form): sections of $\pi_1(X) \to G_k$ (resp. of $G_{k(X)} \to G_k$) arise from rational points of X^c, for X a hyperbolic curve over an infinite field k.

Some results. Voevodsky (1990) investigated this problem in *Etale topologies of schemes over fields of finite type over* $\mathbb{Q}$. Tamagawa: recovering a smooth affine curve X over a finite field from $\pi_1(X)$, if X is hyperbolic - from $\pi_1^t(X)$; also affine hyperbolic curves over finitely generated fields in characteristic zero. Functorially for isomorphisms. Mochizuki: extension to complete hyperbolic curves over finitely generated fields in characteristic zero. Stix: some hyperbolic curves over infinite fields in positive characteristic. Tamagawa: if $X = \mathbb{P}^1_{\bar{\mathbb{F}}_p} \setminus \{0, 1, \infty, x_1, \dots x_n\}$, then it can be recovered from $\pi_1^t(U)$.

2. Origins for the study of $\mathcal{G}_k^c$: unramified Brauer group of $k(V)^G$, after Bogomolov

For a proof as discussed during Talk 1 see J.-L. Colliot-Thélène, *The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group)*, Thm. 6.1, Prop. 4.3, Thm. 7.1, Thm. 7.3 and Example 7.5.

3. Overview of the reading group

3.1. **Talks 2-3.** The main goal is to prove:

Theorem 1. *Let K, K' be function fields of algebraic varieties over algebraically closed fields k, k'. Assume that the transcedence degree of K over k is at least 2. Assume that there exist compatible isomorphisms of abelian groups $\phi_i : \bar{K}_i^M(K) \to \bar{K}_i^M(K'), i = 1, 2$, where $\bar{K}_i^M = K_i^M / \langle$infinitely divisible elements$\rangle$. Then there is an isomorphism of fields $\phi : K \to K'$ compatible with ϕ_1.*

We will in fact discuss a stronger version of this result, when ϕ_1 and ϕ_2 are compatible homomorphisms with ϕ_1 injective, such that its image is not contained in a one-dimensional subfield. Then there exists a homomorphism $\phi : K \to K'$ such that the induced map on $\bar{K}_1^M$ is a rational power of ϕ_1.

This result should hold for any fields K and K' (not necessarily function field over algebraically closed fields k and k').

3.1.1. *TALK 2: elementary theorems on K_1 and K_2.*

a) A motivation for using Milnor K-theory to reconstruct fields. In fact, one can view K_1 as a "dual" discrete analogue of $\mathcal{G}^a$, and K_2 - of $\mathcal{G}^c$. (see section 2 of *Milnor K_2 and field homomorphisms* and section 1 in *Galois theory and projective geometry*) and also the introduction in *Introduction to birational anabelian geometry.*

b) The proof of the reconstruction from the K-theory uses several technical but elementary results from Milnor K-theory and for polynomial rings. For the first one, see section 5 of *Milnor K_2 and field homomorphisms.* For the second one, the key statements are Proposition 11, Theorem 22, as well as formulas (3.12) and (3.13) there in. The proof is quite long and it is probably possible to simplify it. See *Introduction to birational anabelian geometry* for a simplified proof that works in characteristic zero only (proposition 9).

c) An observation: for the K-theory, only these "elementary" results are needed, but for Galois groups more sophisticated tools from the valuation theory are used. Why?

3.1.2. *TALK 3: Abstract projective geometry and reconstruction of fields via K_1^M and K_2^M. Introducing the Galois setting.*

a) A classical reconstruction result allows to reconstruct a field, with its additive and multiplicative structures, from projective geometry:

Theorem 2. *Let K/k and K'/k' be field extensions of degree at least 3 and*

$$S = \mathbb{P}_k(K) \simeq \mathbb{P}_{k'}(K') = S'$$

be a bijection of sets which is an isomorphism of abelian groups and of projective structures. Then $k \simeq k'$ and $K \simeq K'$.

(see *Introduction to birational anabelian geometry*, section 1 and *Galois theory and projective geometry* , section 2.) We first discuss basic notions from the projective geometry and this result.

b) The proof of theorem 1 follows *Milnor K_2 and field homomorphisms*, section 4 and the end of section 5, using the result from the projective geometry above.

c) The setting: $\mathcal{G}_k^c$, ℓ-adic difficulties: section 11 in *Reconstruction of function fields.*

3.2. **Talks 4-7.** The main goal is to prove:

Theorem 3. *Let K, L be function fields over algabraic closures of finite fields k, l respectively, of characteristic different from ℓ. Assume that the transcendence degree of K over k is at least 2 and that there is an isomorphism $\Psi : \mathcal{G}_K^a \xrightarrow{\sim} \mathcal{G}_L^a$ of abelian pro ℓ-groups inducing a bijection of sets Σ_K and Σ_L. Then*

(i) *$k \simeq l$;*

(ii) *there is a unique (up to the composition with a power of the absolute Frobenius automorphism), isomorphism of perfect closures $\bar{\Psi} : \bar{L} \to \bar{K}$, such that $e^{-1}\Psi$ is induced from $\bar{\Psi}$, for some $e \in \mathbb{Z}_\ell^*$.*

The main steps of the reconstruction in the surface case could be described as follows:

a) The first key construction is to obtain, from a subgroup $\sigma \in \Sigma_K$ an inertia element of some valuation. One can then describe the decomposition group, too.

b) From all possible valuations one distinguishes divisorial ones (the idea is that the residue field is not algebraically closed).

c) From a valuation one fixes a choice of an actual divisor: in fact, it is enough to "fix" one.

d) One obtains functions by pairing with divisors (note: we do not fix a model, so that one should consider non-rational divisors as a support).

e) Once we have functions the only remaining step to reduce the reconstruction to the projective geometry case (theorem 2) is to describe which functions are algebraically independent.

Remarks: This result should also work for any algebraically closed field (to do!). The current proof uses that there is no nontrivial valuations on the algebraic closures of $\bar{\mathbb{F}}_p$. For arbitrary algebraically closed field one will have to find a method to separate the valuations coming from the base field from the valuations on K. Also, one needs roots of unity in k (but probably one could relax the condition that k is algebraically closed, too).

3.2.1. *Talk 4.*

- *a)* Valuation theory, as in *Commuting elements in Galois groups of function fields*, sections 2 and 3, and theorem 13 in *Introduction to birational anabelian geometry*. Finding one inertia element: characterisation of "flag functions" (AF-functions), recovering the intertia elements using AF-functions (section 6.3 in *Commuting elements in Galois groups of function fields*).
- *b)* Characterizing decomposition subgroups (Proposition 8.3 in *Reconstruction of function fields*).

3.2.2. *Talk 5.*

- *a)* Choosing divisorial valuations and divisors (remark: see proposition 15.7 in *Reconstruction of function fields*, Proposition 6.4 in *Reconstruction of higher-dimensional function fields*, section 6).
- *b)* Choosing functions: section 12 in *Reconstruction of function fields.*

3.2.3. *Talk 6.* Analysis on curves: sections 13, 14 in *Reconstruction of function fields.*

3.2.4. *Talk 7.* The dimension 2 case: end of proof, following *Reconstruction of function fields*: sections 15 and 16.

3.2.5. *Talk 8.* The general case, following *Reconstruction of higher dimensional function fields.*

3.3. **Talk 9.** If time permits, here we plan to discuss several open questions, in particular the freedom conjecture and the connections with the Block-Kato conjecture. Let $\pi : G_k \to \mathcal{G}_k^a$, $\pi_c : G_k \to \mathcal{G}_k^c$ and $\pi_a : \mathcal{G}_k^c \to \mathcal{G}_k^a$ be the canonical projections. Then:

Theorem 4. *The Bloch-Kato conjecture is equivalent to*

(i) *the map* $\pi^* : H^*(\mathcal{G}_k^a, \mathbb{Z}/\ell^n) \to H^*(\mathcal{G}_k, \mathbb{Z}/\ell^n)$ *is surjective, and*
(ii) *Ker* (π_a^*)=*Ker*(π).

Consider now $\mathfrak{S}_\ell$ an ℓ-Sylow subgroup of G_k and put $\mathfrak{S}_\ell^{(1)} = [\mathfrak{S}_\ell, \mathfrak{S}_\ell]$. The **freeness conjecture** of Bogomolov claims that $H^i(\mathfrak{S}_\ell^{(1)}, \mathbb{Z}/\ell^m) = 0$ for all $i \geq 2$, $n \in \mathbb{N}$. A proof of this conjecture would provide a different proof of the Bloch-Kato conjecture. See *Galois theory and projective geometry,* sections 5 and 6, *Introduction to birational anabelian geomeetry,* section 3.