

MODEL THEORY OF GROUP ACTIONS ON FIELDS

1. INTRODUCTION AND MODEL THEORY OF FIELDS

This lecture is about *algebraic model theory*, which focuses on model-theoretic properties of concrete algebraic structures (as groups, fields, modules etc.). More specifically, we will consider *model theory of fields*, where “field” is understood as “field with a possible extra structure”. We note the following two examples of this extra structure:

- a *derivation* (resulting in the theory DCF);
- an *automorphism* (resulting in the theory ACFA).

These theories will be described to some extent during the lecture. Both of these theories were studied a lot and the model-theoretic knowledge about them has applications in areas outside of model theory as diophantine geometry or algebraic dynamics. We plan to talk about group actions on fields. I will argue that this topic still fits into the framework of two examples given above.

Regarding automorphisms, let us fix a field K . We have the following very general bijection (easy exercise):

$$\text{Aut}(K) \longleftrightarrow \{\text{Actions of } (\mathbb{Z}, +) \text{ on } K \text{ by field automorphisms}\}.$$

Therefore, talking about automorphisms of the field K is the same as talking about actions of the group $(\mathbb{Z}, +)$ on K . In this lecture, we will be interested in actions on fields of *finite* groups and the model theory of such actions. The model theory of infinite group actions is much more involved and it will be briefly mentioned at some point.

Regarding derivations, the situation is more complicated. Derivations of some kind may be still understood as “group” actions, but it has to be properly explained what does “group” mean in this context (for example, a non-trivial “group” may have no non-trivial points!), which is interesting in its own. We will introduce the notion of an *affine finite group scheme*, interpret their actions as derivations of some specific kind, and then discuss the corresponding model theory. At this moment, let me just vaguely say that if a field K has positive characteristic p , then derivations ∂ on K such that $\partial^{(p)} = 0$ (∂ composed with itself p times) are “the same” as actions on K by the kernel of the Frobenius map on the additive group.

I sketch below a rough plan of the lecture (there may be some changes).

- (1) Lecture 1: Introduction and recalling some model theory of pure (that is: without any extra structure) fields.
- (2) Lectures 2–8: Model theory of finite group actions on fields. It will include some notions from infinite Galois theory as: profinite groups, infinite Galois correspondence, Frattini covers. All such notions will be defined.
- (3) Lectures 9–12: A brief introduction to the theory of finite group schemes. This topic formally belongs to algebraic geometry, but it is really about finite dimensional vector spaces with some extra structure. Some elements of category theory will be introduced/recalled here as well.

- (4) Lectures 13–15: Model theory of iterative derivations as finite group scheme actions. We will understand actions of finite group schemes of a special type as some kinds of derivations and then discuss the corresponding model theory.

1.1. Model theory of pure fields. I will recall first some statements from Prof. Newelski’s lecture “Model Theory” (abbreviated by *LN-lecture* in the sequel). I will consider these notions as already known and then add some extra results and comments. We adopt the following convention: n is a fixed (but arbitrary) positive integer, $X = (X_1, \dots, X_n)$ denotes an n -tuple of polynomial variables, and $x = (x_1, \dots, x_n)$ denotes an n -tuple of logical variables.

From LN-lecture.

Let $L_{\text{ring}} = \{0, 1, +, \cdot, -\}$ be the language of rings. We do not have to include “ $-$ ” (it was not included in the LN-lecture), but without it an L_{ring} -substructure of a ring is not necessarily a subring. Let p be a prime number or $p = 0$. Then, ACF_p denotes the L_{ring} -theory whose class of models coincides with the class of algebraically closed fields of characteristic p . The theory ACF_p is complete and has quantifier elimination.

Let K be a subfield of a monster model \mathcal{M} of ACF_p and a be an n -tuple from \mathcal{M} . For a complete type $q \in S_n(K)$, we define:

$$I(a/K) := \{F \in K[X] \mid F(a) = 0\},$$

$$I(q) := \{F \in K[X] \mid “F(x) = 0” \in q\}.$$

Then, there is the following bijection:

$$(\spadesuit) \quad S_n(K) \ni q \mapsto I(q) \in \text{Spec}(K[X])$$

and for all $b \models q$ we have $I(b/K) = I(q)$.

The following is obvious and could have been mentioned at the LN lecture: for a field K , the K -terms in the language of rings are equivalent (modulo the theory of rings) to terms of the form $W(x)$ for some $W \in K[X]$.

Extra results, definitions, and comments (not from LN Lecture).

There is a natural topology on $\text{Spec}(K[X])$ which is described in Problem 1.2. The bijection (\spadesuit) above is continuous, but it is not a homeomorphism ($S_n(K)$ is compact, so how can it happen?). The Stone topology on $S_n(K)$ is richer than the topology on $\text{Spec}(K[X])$, but the topology on $\text{Spec}(K[X])$ is “smarter” than the Stone topology on $S_n(K)$, since it distinguishes definable sets given by polynomial equations as closed sets.

For any field K , there is the Zariski topology on K^n (see Problem 1.1). If Ω is an algebraically closed field, then we sometimes call Zariski closed sets in Ω^n by (affine) *varieties*. If $K \subseteq \Omega$ is a subfield, then we sometimes call K -closed sets in Ω^n (see Problem 1.4) by (affine) K -*varieties*. Irreducible (in the Zariski topology on Ω^n) K -varieties are sometimes called *absolutely irreducible*. This “absolutely” is added here to emphasize that this is a stronger notion than K -irreducibility. For a K -variety $V \subseteq \Omega^n$, there are *three* possible notions of irreducibility:

- K -irreducibility (see Problem 1.5),
- (absolute) irreducibility,

- irreducibility of $V \cap K^n$ (denoted by $V(K)$) in the Zariski topology on K^n .

It is clear that (absolute) irreducibility implies K -irreducibility. Problem 1.5 shows that there are no other implications in general.

By a model-theoretic analysis, we can quickly obtain the following result.

Theorem 1.1 (Weak Hilbert's Nullstellensatz). *Suppose that Ω is an algebraically closed field and I is a proper ideal of $\Omega[X]$ (recall that $X = (X_1, \dots, X_n)$). Then, there is $a \in \Omega^n$ such that for all $F \in I$ we have $F(a) = 0$.*

Proof. Let $F_1, \dots, F_r \in I$ be such that $I = (F_1, \dots, F_r)$ (Hilbert's Basissatz). It is enough to find $a \in \Omega^n$ such that $F_1(a) = \dots = F_r(a) = 0$. Since $I \neq \Omega[X]$, I extends to a maximal ideal $\mathfrak{m} \trianglelefteq \Omega[X]$. Let $L := \Omega[X]/\mathfrak{m}$ (it is a field) and $\Phi : \Omega \rightarrow L$ denote the following composition:

$$\Omega \xrightarrow{\subseteq} \Omega[X] \longrightarrow \Omega[X]/\mathfrak{m} = L.$$

Since Φ is a homomorphism of fields, it is an embedding. Hence we can identify Ω with a subfield of L . Let

$$v := (X_1 + \mathfrak{m}, \dots, X_n + \mathfrak{m}) \in L^n.$$

It is easy to check (but some care is necessary) that

$$F_1(v) = \dots = F_r(v) = 0.$$

Let L^{alg} denote the algebraic closure of L . We have that:

$$L^{\text{alg}} \models (\exists x)(F_1(x) = 0 \wedge \dots \wedge F_r(x) = 0).$$

Let $p := \text{char}(\Omega)$. Since the theory ACF_p has quantifier elimination, the field extension $\Omega \subseteq L^{\text{alg}}$ is elementary and we have:

$$\Omega \models (\exists x)(F_1(x) = 0 \wedge \dots \wedge F_r(x) = 0).$$

Therefore, there is $a \in \Omega^n$ such that $F_1(a) = \dots = F_r(a) = 0$, which finishes the proof. \square

We still assume that Ω is an algebraically closed field. For a Zariski closed subset $V \subseteq \Omega^n$, let us denote:

$$I(V) := \{F \in \Omega[X] \mid F(V) = 0\}.$$

For a K -closed subset $V \subseteq \Omega^n$, let us denote:

$$I_K(V) := \{F \in K[X] \mid F(V) = 0\} = I(V) \cap K[X].$$

Using Weak Nullstellensatz, one can show the following (we will come back to these proofs later).

- (1) (Hilbert's Nullstellensatz) For any $A \subseteq \Omega[X]$, we have (see Problem 1.1 for the definition of $Z(A)$):

$$I(Z(A)) = \sqrt{(A)},$$

where $\sqrt{(A)}$ denotes the radical of the ideal of $\Omega[X]$ generated by A .

- (2) For a Zariski closed subset $V \subseteq \Omega^n$, we have that V is irreducible if and only if the ideal $I(V)$ is prime in the ring $\Omega[X]$.
- (3) For a K -closed subset $V \subseteq \Omega^n$, we have that V is K -irreducible if and only if the ideal $I_K(V)$ is prime in the ring $K[X]$.

Problem List 1

Let Ω be a field, K is a subfield of Ω , $n > 0$, and $X = (X_1, \dots, X_n)$.

- (1) Let $A \subseteq \Omega[X]$. We define:

$$Z(A) := \{a \in \Omega^n \mid (\forall F \in A)(F(a) = 0)\}.$$

Show the following.

- (a) The sets of the form $Z(A)$ are the closed sets of a topology on Ω^n , which is called the *Zariski topology*.
 - (b) The topological space from Item (a) above is *Noetherian*, that is each decreasing sequence of closed subsets stabilizes.
 - (c) A subspace of an arbitrary Noetherian topological space is again Noetherian (with the induced topology).
 - (d) Each Noetherian topological space decomposes into a finite number of *irreducible* closed subsets, that is subsets that can not be presented as a non-trivial union of two closed subsets.
- (2) Let R be a commutative ring with 1 and let $\text{Spec}(R)$ be the set of all prime ideals of R . For $I \trianglelefteq R$, we define:

$$V(I) = \{P \in \text{Spec}(R) \mid I \subseteq P\}.$$

Let $P \in \text{Spec}(R)$. Show the following.

- (a) The sets of the form $V(I)$ are the closed sets of a topology on $\text{Spec}(R)$.
 - (b) The singleton $\{P\}$ is closed if and only P is a maximal ideal.
- (3) Show that the following map:

$$\Psi : \Omega^n \rightarrow \text{Spec}(\Omega[X]), \quad \Psi(a_1, \dots, a_n) = (X_1 - a_1, \dots, X_n - a_n) \triangleleft \Omega[X]$$

is a homeomorphism between Ω^n (with the Zariski topology) and $\Psi(\Omega^n)$ (with the subspace topology induced from $\text{Spec}(\Omega[X])$).

- (4) A closed subset $V \subseteq \Omega^n$ is *K-closed*, if there is $A \subseteq K[X]$ such that $V = Z(A)$. For a *K-closed* $V \subseteq \Omega^n$, we denote $V(K) := V \cap K^n$. Show the following.
- (a) The *K-closed* sets are the closed sets of a Noetherian topology on Ω^n .
 - (b) The subspace topology on K^n induced from Ω^n with the *K-closed* set topology from Item (a) coincides with the Zariski topology on K^n .
 - (c) The subspace topology on K^n induced from Ω^n with the Zariski topology coincides with the Zariski topology on K^n . That is: for any closed subset $V \subseteq \Omega^n$, there is a *K-closed* subset $V_K \subseteq \Omega^n$ such that $V(K) = V_K(K)$.
(Find an elementary algebraic proof, don't use model-theoretic stability.)
- (5) A *K-closed* set is *K-irreducible*, if it is an irreducible set in the topology from Problem (4a). Find the following examples of K, Ω and *K-closed* $V \subseteq \Omega^n$.
- (a) V is *K-irreducible* and V is not irreducible.
 - (b) V is irreducible and $V(K)$ is not empty and not irreducible (in K^n).
 - (c) V is not *K-irreducible* and $V(K)$ is not empty and irreducible (in K^n).

2. MODEL COMPANION AND MODEL-THEORETIC SET-UP FOR GROUP ACTIONS

2.1. Model companion. Let L be a language, κ be a cardinal number and suppose that for each $i < \kappa$, there is an L -structure M_i . We say that $(M_i)_{i < \kappa}$ is a *chain of L -structures*, if for each $i < j$, we have that M_i is an L -substructure of M_j . It is clear that if $(M_i)_{i < \kappa}$ is a chain of L -structures, then the increasing union

$$M := \bigcup_{i < \kappa} M_i$$

has a unique L -structure such that each M_i is an L -substructure of M .

Let T be an L -theory. We say that $(M_i)_{i < \kappa}$ is a *chain of models of T* , if it is a chain of L -structures and each M_i is a model of T .

Definition 2.1. The theory T is *inductive*, if for each chain of models of T , its union is also a model of T .

A $\forall\exists$ -*formula* is a formula of the form $\forall x\exists y\varphi(x, y, z)$, where $\varphi(x, y, z)$ is a quantifier-free formula and x, y, z are tuples of variables.

An L -theory T is a $\forall\exists$ -*theory*, if there is an L -theory T' such that T' consists of $\forall\exists$ -sentences and T' is equivalent to T (that is: the class of models of T coincides with the class of models of T' ; in short: “ T and T' have the same models”).

Proposition 2.2. *A theory is inductive if and only if it is a $\forall\exists$ -theory.*

Problem 2.1 asks for a proof of the right-to-left implication. We skip a proof of the left-to-right implication, since all the theories considered in this lecture will be $\forall\exists$ -theories.

Definition 2.3. Let $M \models T$. We say that M is an *existentially closed* (abbreviated *e.c.*) model of T , if for any quantifier free L_M -formula $\chi(x)$ and any L -extension $M \subseteq N$ of models of T , we have that:

$$N \models \exists x\chi(x) \quad \text{implies} \quad M \models \exists x\chi(x).$$

Intuitively, all solvable in an extension of M “systems of (in)equations” (represented by a quantifier-free formula) can be already solved in M (Hodges: “Existentially closed structures are one of those happy ideas which occur to several different mathematicians at different times and places, beginning with those Renaissance scholars who invented imaginary numbers.”).

We will use the following natural convention. If, for example, we say: “ G is an e.c. group”, then we mean “ G is an e.c. model of the theory of groups”. Similarly for rings, fields etc.

Example 2.4. We will show that the class of existentially closed fields (or domains) coincides with the class of algebraically closed fields. It is clear that any existentially closed field is algebraically closed, since any polynomial of positive degree with coefficients from a field F has a zero in a field extension of F .

For the opposite implication, let F be an algebraically closed field and we will show that F is existentially closed. Let $\varphi(x)$ be a quantifier-free L_F -formula and $F \subseteq K$ be a field extension such that $K \models \exists x\varphi(x)$. We need to show that $F \models \exists x\varphi(x)$. Since $\varphi(x)$ is quantifier-free, it is a Boolean combination of atomic formulas. By the form of

terms in the language L_F , the atomic formulas in L_F are equivalent (modulo the theory of rings) to ones of the form “ $W(x) = 0$ ”, where $W \in F[X]$. For any field extension $F \subseteq M$ and any $a \in M^n$, we clearly have that:

$$(\spadesuit) \quad M \models \neg(W(a) = 0) \quad \text{if and only if} \quad M \models (W(a)W(a)^{-1} = 1).$$

We replace any atomic formula of the form “ $\neg(W(x) = 0)$ ” in $\varphi(x)$ with the formula “ $W(x)t = 1$ ”, where t is a new variable and we obtain in this way a new quantifier free formula $\varphi'(x, t)$ without negations of atomic formulas. By (\spadesuit) , we get that:

$$M \models \exists x \varphi(x) \quad \text{if and only if} \quad M \models \exists x \exists t \varphi'(x, t).$$

Therefore, we can replace in this proof $\varphi(x)$ with $\varphi(x, t)$ and assume without loss of generality that $\varphi(x)$ does not contain negations of atomic formulas (“Rabinowitsch trick”). We can also assume that $\varphi(x)$ does not have any disjunctions and as a result $\varphi(x)$ is of the form: “ $W_1(x) = 0 \wedge \dots \wedge W_r(x) = 0$ ” for some $W_1, \dots, W_r \in F[X]$. Since $K \models \exists x \varphi(x)$, we get that

$$I := (W_1, \dots, W_r)F[X] \neq F[X]$$

(otherwise we would get $K \models (1 = 0)$). By Weak Hilbert’s Nullstellensatz (Theorem 1.1), the ideal I has a zero in F . In particular, we obtain $F \models \exists x \varphi(x)$, which finishes the proof.

Remark 2.5. Using quantifier elimination for the theory ACF_p (where $p = \text{char}(F)$), one could conclude the proof from Example 2.4 in the following, much quicker, way. By quantifier elimination, the field extension $F \subseteq K^{\text{alg}}$ is elementary. Since $K \models \exists x \varphi(x)$ and $\varphi(x)$ is quantifier-free, we also get $K^{\text{alg}} \models \exists x \varphi(x)$. Since the field extension $F \subseteq K^{\text{alg}}$ is elementary, we get $F \models \exists x \varphi(x)$.

However, the more complicated proof from Example 2.4 will be useful in situations where we do not have any theory with quantifier-elimination “at hand” and this is the situation one usually encounters.

Lemma 2.6. *Assume that T is inductive and $M \models T$. Then, there is an L -extension $M \subseteq N$ such that N is an e.c. model of T .*

The proof of Lemma 2.6 is similar to the proof of existence of an algebraic closure of a field, but it is even simpler: in the case of fields, for a given non-constant polynomial $W \in F[X]$ in a single variable one has to construct a field extension $F \subseteq K$ such that W has a zero in K and then use induction. In our case, for any “solvable” quantifier-free formula, we already have an extension, so we need only to use (transfinite) induction which is left as Problem 2.2.

By Lemma 2.6, existentially closed models exists. We give below a definition of the notion of a model companion in a form which is convenient for us.

Definition 2.7. For an inductive L -theory T , we call an L -theory T^* a *model companion* of T if the class of models of T^* coincides with the class of e.c. models of T .

Remark 2.8. A class of L -structures is *elementary*, if there is an L -theory T' such that this class coincides with the class of models of T' . Therefore, for an inductive theory T , T has a model companion if and only if the class of e.c. models of T is elementary (and the model companion coincides with the axiomatization of this class).

We recall that a theory T is *model complete* if every L -extension of models of T is elementary.

Remark 2.9. Let T be an arbitrary L -theory. We collect some general definitions and results without proofs.

- (1) A *companion* of T is a theory T' such that every model of T can be embedded in a model of T' , and every model of T' can be embedded in a model of T .
- (2) A *model companion* is a companion which is model complete. It was shown by Robinson that any theory has at most one model companion.
- (3) For inductive theories, the above definition coincides with Definition 2.7.

Let us recall that an L -structure M is κ -saturated, if

- for all $A \subseteq M$ such that $|A| < \kappa$,
- for all finitely satisfiable in M sets of L_A -formulas $p(x)$ (in other words: types in M over A);

the type $p(x)$ is satisfiable in M . We say that M is a κ -saturated model of T , if $M \models T$ and M is a κ -saturated L -structure.

Remark 2.10. If T is inductive, then it has e.c. models. For any cardinal κ , an arbitrary theory T has κ -saturated models. Therefore, if T has a model companion, then T also has κ -saturated e.c. models, so it has “very big models”.

Example 2.11. Model companions and non-companionable theories (Hodges: “There are many examples of non-companionable theories, but most of them depend on substantial mathematics”).

- (1) The theory of sets has a model companion, which is the theory of infinite sets (Problem 2.3).
- (2) The theory of linear orders has a model companion, which is the theory of dense linear orders without end-points (Problem 2.4).
- (3) By Example 2.4, the theory of fields has a model companion, which is the theory of algebraically closed fields.
- (4) The theory of *difference* (or *transformational*) fields (that is: fields with an automorphism) has a model companion, which is called ACFA. The axioms will be discussed later.
- (5) The theory of *differential* fields (that is: fields with a derivation) has a model companion, which is called DCF. The axioms will be discussed later.
- (6) The theory of commutative groups has a model companion, which is the theory of commutative divisible groups having infinitely many elements of order p for every prime p (Problem 2.7).
- (7) The theory of groups has no model companion.

Proof. Suppose that the theory of groups has a model companion and we will reach a contradiction. Let G be a “monster model” of this model companion, that is an e.c. group, which is κ -saturated and κ -strongly homogenous for some $\kappa > \mathfrak{c}$. There are at most continuum orbits of the action of $\text{Aut}(G)$ on G , since there are at most continuum 1-types over empty set calculated in G . By Problem 2.8(a), there are at most continuum conjugacy classes in G . Using this

and the κ -saturation of G , we get that there are finitely many conjugacy classes in G , which contradicts Problem 2.8(c). \square

It can be shown that every e.c. group is “ultrahomogeneous”; that is: every isomorphism between finitely generated subgroups extends to an inner automorphism.

- (8) The theory of commutative rings has no model companion.

Proof. It is enough to show that a non-principal ultrapower of an e.c. commutative ring is not e.c.

Let A be an e.c. commutative ring and assume that:

$${}^*A := \prod_I A/\mathcal{U}$$

is e.c. We will reach a contradiction. Since A is e.c., for each $n > 0$ there is $r_n \in A$ such that $r_n^{n-1} \neq 0 = r_n^n$ (nilpotent of degree n). Let

$$r := (r_n)_n/\mathcal{U} \in {}^*A.$$

By Łoś Theorem, r is not nilpotent. By Problem 2.9(a), there is a ring extension ${}^*A \subseteq B$ and an idempotent element $b \in B$ such that r divides b in B . Since *A is e.c., there is an idempotent element $a \in {}^*A$ such that r divides a in A . By Łoś Theorem again, there is $n > 0$ (even infinitely many n 's) such that there is an idempotent element $a_n \in A$ such that r_n divides a_n in A . By Problem 2.9(a), r_n is not nilpotent, a contradiction. \square

In Problem 2.9(b), you are asked to transform (“to un-Łoś”) the above proof to show that there is no \aleph_0 -saturated and existentially closed commutative ring.

If we want to study model-theoretic properties of some axiomatizable objects (as differential fields, ordered sets or group actions on fields), it is natural to start from a model companion of the corresponding theory (if it exists). Then, we get a nice model complete theory of “large” objects of the kind we are interested in. Hence, the first natural question in this context is: does a model companion of a given theory exist? A large part of this lecture is related to this question in the case of group actions on fields.

2.2. Model-theoretic set-up for group actions on fields. Let us fix a group G , we will usually denote the group operation in G by “nothing”, that is hg for $h, g \in G$, and the neutral element is denoted by e . We use the following (not very standard) terminology: we call a pair consisting of a ring together with a G -action on this ring by G -ring. Similarly, we consider G -fields, G -ring/ G -field extensions, etc.

We define the following *language of G -rings*:

$$L_G := L_{\text{ring}} \cup \{\lambda_g \mid g \in G\},$$

where each λ_g is a unary function symbol. Then, the theory of G -fields, abbreviated G – TF, is the following:

$$\begin{aligned} G - \text{TF} := & \text{Theory of fields} \cup \{\lambda_g \circ \lambda_h = \lambda_{gh} \mid g, h \in G\} \cup \{\lambda_e = \text{id}_G\} \\ & \cup \{\lambda_g \text{ is a field automorphism} \mid g \in G\}. \end{aligned}$$

It is clear that the class of models of the theory $G - \text{TF}$ coincides with the class of G -fields after the identification ($g \in G, a \in K$):

$$\varphi : G \longrightarrow \text{Aut}(K), \quad \lambda_g(a) = \varphi(g)(a) (= g \cdot a).$$

Remark 2.12. It is often more natural and more convenient to consider the language coming from a chosen set of generators of the group G . For example, if $G = \mathbb{Z}$, then the natural language is $L_\sigma := L_{\text{ring}} \cup \{\sigma\}$, where σ is a unary function symbol corresponding to a generator of the group \mathbb{Z} . This is the language of *difference rings*, that is rings with an automorphism.

As mentioned in the previous subsection, the main question is: does a model companion of the theory $G - \text{TF}$ exist?

Example 2.13. We give one positive and one negative example.

- (1) If $G = \mathbb{Z}$, then $G - \text{TF}$ corresponds to the theory of difference fields and a model companion exists (the theory ACFA).
- (2) If $G = \mathbb{Z} \times \mathbb{Z}$, then $G - \text{TF}$ corresponds to the theory of fields with two commuting automorphisms. Quite surprisingly, the model companion does not exist (Hrushovski).

If we drop the commutativity assumption (that is, we consider actions of the free group F_2), then a model companion exists.

Characterizing the class of groups G such that a model companion of the theory $G - \text{TF}$ exists seems to be a very hard problem, it is not even clear what an answer should be. I will comment more on this later, after we learn some model theory of finite group actions on fields.

Problem List 2

For $k > 0$, C_k denotes the cyclic group of order k . Let \mathbb{P} denote the set of prime numbers. For an Abelian group A and $p \in \mathbb{P}$, we define the following subgroups of A :

$$A[k] := \{a \in A \mid ka = 0\}, \quad A[p^\infty] = \bigcup_{n=1}^{\infty} A[p^n].$$

- (1) Show that if T is an $\forall\exists$ -theory, then for each chain of models of T , its union is also a model of T .
- (2) Show that any model of an inductive theory T extends to an e.c. model of T .
- (3) Show that the theory of infinite sets is a model companion of the theory of sets (the empty theory in the language of equality).
- (4) Show that the theory of densely linearly ordered sets without end-points is a model companion of the theory of linearly ordered sets.
- (5) Show that any e.c. domain is an algebraically closed field.
- (6) If $k|l$, then we regard C_k as a subgroup of C_l . For $p \in \mathbb{P}$, show the following:

$$\mathbb{C}^*[p^\infty] \cong \bigcup_{n=1}^{\infty} C_{p^n} \cong (\mathbb{Q}/\mathbb{Z})[p^\infty].$$

We denote $C_{p^\infty} := \bigcup_{n=1}^{\infty} C_{p^n}$ and call it the *Prüfer p -group*.

- (7) Let A be a commutative group. Show the following.
 - (a) The group A is divisible if and only if we have

$$A \cong \mathbb{Q}^{\oplus \kappa} \oplus \bigoplus_{p \in \mathbb{P}} (C_{p^\infty})^{\oplus \kappa_p},$$

where κ, κ_p are cardinal numbers and, for example, $\mathbb{Q}^{\oplus \kappa}$ stands for $\bigoplus_{i < \kappa} \mathbb{Q}$.

- (b) For a fixed commutative divisible group A , the cardinal numbers κ, κ_p from Item (a) are unique. The *Prüfer p -rank* of A is defined as κ_p .
- (c) If A is divisible, then for any $p \in \mathbb{P}$, the Prüfer p -rank of A coincides with $\dim_{\mathbb{F}_p}(A[p])$ ($A[p]$ has the obvious structure of a vector space over \mathbb{F}_p).
- (d) There is a theory T_∞ whose models are divisible commutative groups having infinite Prüfer p -rank for all $p \in \mathbb{P}$.
- (e) There is $B \models T_\infty$ and a monomorphism $A \rightarrow B$.
- (f) If A is divisible and $A \leq B$ is a group extension, then there is $A' \leq B$ such that $B = A \oplus A'$.
- (g) The theory T_∞ is a model companion of the theory of commutative groups.
- (8) Suppose that G is an e.c. group and $a, b \in G$. Show the following.
 - (a) If there is $f \in \text{Aut}(G)$ such that $f(a) = b$, then a and b are conjugate in G .
 - (b) For any $k > 0$, there is an element of order k in G .
 - (c) The group G has infinitely many conjugacy classes.
- (9) Let R be a commutative ring and $r \in R$.
 - (a) Show that r is not nilpotent if and only if there is a ring extension $R \subseteq S$ and a non-zero idempotent $s \in S$ ($s^2 = s$) such that r divides s in S .
 - (b) Show that there is no \aleph_0 -saturated e.c. commutative ring.
- (10) Show that the class of non-algebraically closed fields is not elementary.

3. FINITE GALOIS THEORY AND ACTIONS OF FINITE GROUPS

3.1. Finite Galois theory. I collect below some facts related with finite Galois theory, which I assume you already know.

For a field K , K^{sep} denotes a fixed separable closure of K and K^{alg} denotes a fixed algebraic closure (containing K^{sep}) of K . For any $k > 0$, C_k denotes a cyclic group of order k . If $K \subseteq L$ is a Galois field extension (so far, finite), then $\text{Gal}(L/K)$ denotes $\text{Aut}(L/K)$, that is the field automorphisms of L fixing K pointwise. For $l > 0$, $\zeta_l \in K^{\text{sep}}$ denotes a primitive l -th root of unity (it exists if and only if $\text{char}(K) \nmid l$). If a group G acts on K by field automorphisms, then we define:

$$K^G := \{x \in K \mid (\forall g \in G)(g \cdot x = x)\},$$

which is the *subfield of invariants*. If the group G is moreover finite and the action of G on K is faithful, then the field extension $K^G \subseteq K$ is Galois of degree $|G|$ (the order of G).

Let p be a prime number.

The following result describes Galois extensions of degree p in the case when p is not the characteristic (and one more condition is satisfied). There are more general versions of the result below, but we focus on a version we will need later.

Theorem 3.1 (Kummer theory of cyclic extensions). *Let $F \subseteq C$ be a Galois extension of degree p such that $\text{char}(F) \neq p$. Assume moreover that $\zeta_p \in F$. Then, there is $\gamma \in C$ such that $C = F(\gamma)$ and $\gamma^p \in F$.*

One formal comment: for any $n > 0$, if ζ, ζ' are n -th primitive roots of unity, then ζ' is a power of ζ (and vice-versa), so for any appropriate field K , we have:

$$\zeta \in K \iff \zeta' \in K,$$

hence the statement “ $\zeta_n \in K$ ” is unambiguous.

The following result describes Galois extensions of degree p in the case when p coincides with the characteristic.

Theorem 3.2 (Artin-Schreier theory of cyclic extensions). *Let $F \subseteq C$ be a Galois extension of degree p such that $\text{char}(F) = p$. Then, there is $\gamma \in C$ such that $C = F(\gamma)$ and $\gamma^p - \gamma \in F$.*

3.2. Actions of finite groups. We assume that G is a finite group of cardinality k and we write

$$G = \{g_1 = e, g_2, \dots, g_k\}.$$

Example 3.3. If the group G is trivial, then the class of G -fields coincides with the class of fields, hence a model companion exists and it coincides with the theory ACF.

From now on, we assume that G is non-trivial, which will be sometimes explicitly recalled. To fix our intuitions, we consider first actions on algebraically closed fields. Recall that if a finite group G acts on K , then the field extension $K^G \subseteq K$ is finite, so the following classical result is very relevant here.

Theorem 3.4 (Artin-Schreier). *Let F be a field whose algebraic closure is a finite proper extension. Then F has characteristic 0 and its algebraic closure is the quadratic extension $F(i)$.*

Before the proof, let us discuss some consequences. By Theorem 3.4, we get that if a finite non-trivial group G acts faithfully on an algebraically closed field K , then $\text{char}(K) = 0$ and $G = C_2$ (we apply Theorem 3.4 for $F := K^G$). We will see below that this unique possibility still does not yield an existentially closed C_2 -field.

Example 3.5. The field \mathbb{C} with the complex conjugation σ is clearly a C_2 -field, since $\sigma^2 = \text{id}$. We will see below that (\mathbb{C}, σ) is not an existentially closed C_2 -field. We consider the following “difference equation”:

$$x\sigma(x) = -1.$$

It has no solutions in the C_2 -field (\mathbb{C}, σ) , since for any $z \in \mathbb{C}$ we have:

$$z\sigma(z) = |z|^2 \geq 0.$$

But it has a solution (for example: X) in the following C_2 -field extension:

$$(\mathbb{C}(X), \tilde{\sigma}), \quad \tilde{\sigma}(X) = -1/X$$

(by Problem 3.6, there is a unique such C_2 -field extension).

Having the above information, one can show that if K is an existentially closed G -field (G finite and non-trivial), then K is *not* algebraically (and even separably) closed (Problem 3.8). So, what kind of fields we obtain as (the underlying fields) of G -fields for G as above? We will learn the answer during the next lectures.

Our presentation of the proof of Theorem 3.4 follows Conrad’s notes: <https://kconrad.math.uconn.edu/blurbs/galoistheory/artinschreier.pdf> and many steps are left for problem sessions. It is convenient to separate the following important partial result.

Proposition 3.6. *Let $F \subseteq C$ be a Galois extension such that $[C : F] = p$ is a prime number and the field C is algebraically closed. Then, we have the following:*

- (i) $p = 2$,
- (ii) $\text{char}(C) \neq 2$,
- (iii) $i := \zeta_4 = \sqrt{-1} \notin F$.

Proof. We show first that $\text{char}(C) \neq p$. Assume that $\text{char}(C) = p$ and we will reach a contradiction. By Theorem 3.2, there is $a \in F$ such that $C = F(\alpha)$, where α is a root of the irreducible polynomial $X^p - X - a \in F[X]$. Any $b \in C$ can be uniquely written as:

$$b = b_0 + b_1\alpha + \dots + b_{p-1}\alpha^{p-1}$$

for some $b_0, \dots, b_{p-1} \in F$. Then, it can be computed that:

$$b^p - b = ((b_{p-1})^p - b_{p-1})\alpha^{p-1} + \text{lower degree terms in } \alpha.$$

Take $b \in C$ such that $a\alpha^{p-1} = b^p - b$ (such b exists, since C is algebraically closed). Then we have (for b_i as above, which are related to our choice of b):

$$a\alpha^{p-1} = ((b_{p-1})^p - b_{p-1})\alpha^{p-1} + \text{lower degree terms in } \alpha.$$

By uniqueness of the coefficients above, we get that $a = (b_{p-1})^p - b_{p-1}$. Hence $b_{p-1} \in F$ is a root of the irreducible polynomial $X^p - X - a \in F[X]$, which is a contradiction by Bezout’s Theorem.

We have shown that $\text{char}(C) \neq p$ and we proceed now with the main argument, that is we aim to show that $p = 2$ which will give us Items (i) and (ii). Since C is an algebraically closed field and $\text{char}(C) \neq p$, we obtain that $\zeta_p \in C$. Since $[F(\zeta_p) : F] \leq p - 1$ and $[C : F] = p$ is a prime number, we get that $\zeta_p \in F$. By Theorem 3.1, there is $\gamma \in C$ such that $C = F(\gamma)$ and $\gamma^p \in F$.

Let σ be a generator of the Galois group $\text{Gal}(C/F)$ and $\beta \in C$ be such that $\beta^p = \gamma$. Since $\beta^{p^2} = \gamma^p \in F$, we obtain the following:

$$\beta^{p^2} = \sigma(\beta^{p^2}) = (\sigma(\beta))^{p^2}.$$

Therefore, there is $\omega \in C$ such that $\omega^{p^2} = 1$ and:

$$(1) \quad \sigma(\beta) = \omega\beta.$$

Since ω^p is a p -th root of unity, arguing as we did above for ζ_p , we obtain $\omega^p \in F$, which implies that $(\sigma(\omega)/\omega)^p = 1$.

If $\omega^p = 1$, then we get a contradiction since it implies $\sigma(\beta^p) = \beta^p$, so $\gamma = \beta^p \in F$ and $C = F(\gamma) = F$. Hence ω^p is a primitive p -th root of unity. Since ω^p is a primitive p -th root of unity and $\sigma(\omega)/\omega$ is a p -th root of unity, there is $k \in \mathbb{Z}$ such that $\sigma(\omega)/\omega = (\omega^p)^k$, that is:

$$(2) \quad \sigma(\omega) = \omega^{1+pk}.$$

From (1) and (2), we obtain the following (for $n \geq 0$, σ^n denotes σ composed with itself n times):

$$\begin{aligned} \beta &= \sigma^p(\beta) \\ &= \omega\sigma(\omega) \dots \sigma^{p-1}(\omega)\beta \\ &= \omega^{1+(1+pk)+\dots+(1+pk)^{p-1}}\beta. \end{aligned}$$

Since the multiplicative order of ω is p^2 , we get the following congruences modulo p^2 (the last one is even the equality):

$$\begin{aligned} 0 &\equiv \sum_{j=0}^{p-1} (1 + pk)^j \\ &\equiv \sum_{j=0}^{p-1} (1 + jpk) \\ &\equiv p + \frac{p(p-1)}{2}pk. \end{aligned}$$

This implies that p divides $1 + kp(p-1)/2$, hence $p = 2$ and k is odd, so we have shown Items (i) and (ii).

It remains to show Item (iii) saying that $i \notin F$. Since $p = 2$, ω has multiplicative order 4. Hence $\omega = i$ and we get the following (since k is odd):

$$\sigma(\omega) = \omega^{1+2k} = \omega^3 \neq \omega.$$

Therefore, we get that

$$\omega = i \notin F = \text{Fix}(\sigma),$$

which finishes the proof. □

We can conclude now the proof of the Artin-Schreier Theorem.

Proof of Theorem 3.4. Let $C := F^{\text{alg}}$. By Problem 3.3, the field extension $F \subseteq C$ is Galois. The main point in this proof is to show the following.

Claim

$$[C : F] = 2.$$

Proof of Claim. Let us assume that $[C : F] \neq 2$ and we will reach a contradiction. Since $[C : F] \neq 2$, we get that $t|[C : F]$, where $t = 4$ or t is an odd prime. Since $\text{Gal}(C/F) = [C : F]$, we get by the Sylow theorems that there is $H \leq \text{Gal}(C/F)$ such that $|H| = t$. Let us set $K := C^H$. By Galois theory, we get $[C : K] = t$. By Proposition 3.6(i), we obtain that t can not be an odd prime, so $t = 4$.

Since

$$|\text{Gal}(C/K)| = [C : K] = t = 4,$$

$\text{Gal}(C/K)$ has a subgroup of order 2. By Galois theory again, there is a tower of fields $K \subset K' \subset C$ such that $[C : K'] = 2$. By Proposition 3.6(iii), we obtain that $i \notin K'$, therefore $i \notin K$. But then $[C : K(i)] = 2$ and by Proposition 3.6(iii) again we get that $i \notin K(i)$, which is a contradiction finishing the proof of Claim. \square

By Proposition 3.6 (and Claim), $\text{char}(F) \neq 2$ and $i \notin F$. Since the field $C = F(i)$ is algebraically closed, we get that every element of $F(i)$ is a square in $F(i)$. Therefore, the assumption from Problem 3.4 are satisfied and by Problem 3.4(b), we get that F has characteristic 0, which finishes the proof of Theorem 3.4. \square

- Remark 3.7.**
- (1) It can be shown that “algebraically closed” from the statement of Theorem 3.4 can be replaced with “separably closed” there.
 - (2) Problem 3.5 shows that any F from the statement of Theorem 3.4 “looks like \mathbb{R} ”, that is F is an *ordered field* whose positive elements are non-zero squares. Actually, such an F is a *real closed field*, so F and \mathbb{R} are elementary equivalent (we will not prove it).
 - (3) There are “non-standard” fields F as in the statement of Theorem 3.4 of arbitrary infinite cardinality (Problem 3.10).

Problem List 3

Let G be a group and $i = \zeta_4$ denote a 4-th primitive root of unity.

- (1) Let F be a field of characteristic $p > 0$, $a \in F$, and $m \in \mathbb{N}$. Show that if a is not a p -th power in F , then the polynomial $X^{p^m} - a$ is irreducible in $F[X]$.
- (2) Suppose that $F \subseteq K$ is a field extension such that F is not perfect and K is perfect. Show that this extension is infinite.
- (3) Let $F \subseteq C$ be a finite field extension such that the field C is algebraically closed. Show that this field extension is Galois.
You are not allowed to use the Artin-Schreier Theorem in this proof!
- (4) Suppose that F is a field such that:
 - $\text{char}(F) \neq 2$;
 - $i \notin F$;
 - every element of $F(i)$ is a square in $F(i)$.

Show the following.

- (a) Every finite sum of squares in F is a square in F .
- (b) The field F has characteristic 0.
- (5) Let F be a field of characteristic 0 such that $i \notin F$ and $F(i)$ is an algebraically closed field.
 - (a) Show that for every $a \in F^*$, exactly one of a and $-a$ is a square.
 - (b) Show that if $a_1, \dots, a_n \in F^*$ ($n > 0$) are squares, then $a_1 + \dots + a_n$ is a non-zero square.
 - (c) Give the definition of an *ordered field* $(K, <)$.
 - (d) Show that F becomes an ordered field with the order defined as:

$$a \leq b \quad \iff \quad b - a \text{ is a square.}$$

- (6) Let $\sigma \in \text{Aut}(\mathbb{C})$ be the complex conjugation. Show the following.
 - (a) There is a unique $\tilde{\sigma} \in \text{Aut}(\mathbb{C}(X))$ such that $\tilde{\sigma}(X) = -1/X$ and for any $z \in \mathbb{C}$ we have $\tilde{\sigma}(z) = \sigma(z)$.
 - (b) For $\tilde{\sigma}$ from Item (a) above, we have $\tilde{\sigma} \circ \tilde{\sigma} = \text{id}$.
- (7) Suppose that K is an existentially closed G -field. Show that the field K is perfect (G need not be finite here).
- (8) Suppose that K is an existentially closed G -field and G is finite. Show the following.
 - (a) The field K is not algebraically closed.
 - (b) The field K is not separably closed.
- (9) Let L be a language, κ be a cardinal number and M be a κ -saturated L -structure.
 - (a) Give the definition of a consistent type in variables $(x_i)_{i < \kappa}$.
 - (b) Let $p(x_i)_{i < \kappa}$ be a consistent type (with respect to the theory $\text{Th}(M)$) in variables $(x_i)_{i < \kappa}$. Show that p has a realization in M .
 - (c) Suppose that L is the language of groups. Write down a type $p(x_i)_{i < \kappa}$ expressing the property that there are at least κ different conjugacy classes.
- (10) Show that for every infinite cardinal number κ , there is an algebraically closed field C such that $|C| = \kappa$ and C has an automorphism of order 2.

4. INFINITE GALOIS THEORY

It may seem strange that to understand the model theory of actions of *finite* groups on fields, we need to know some Galois theory of *infinite* Galois extensions. The reason comes from the last lecture: if an action of a finite group G on a field K is “interesting”, then K has arbitrarily large finite field extensions and we need to understand them all (they are first-order interpretable in the field K). The best think to do is to understand the entire infinite Galois field extension $K \subseteq K^{\text{sep}}$ and exactly for this purpose we need the infinite Galois theory.

I will present necessary results and definitions from the Galois theory of infinite algebraic extensions. The crucial notion here is the notion of a *profinite group*, which is a *topological group* of a special type.

Let us start with a general example which is crucial for us. We will also give an explicit example of this situation to understand all the related concepts better. At the same time, we will also state some formal definitions related to this general example. Assume that $K \subseteq M$ is a Galois field extension (possibly infinite) and $\text{Gal}(M/K)$ is its Galois group (possibly infinite).

Example 4.1. As an explicit example, we take a prime field of positive characteristic $K := \mathbb{F}_p$ and $M := \mathbb{F}_p^{\text{alg}}$. The choice of the prime number p does not matter here.

The above example fits into the following general definition.

Definition 4.2. Let F be a field. We denote:

$$\text{Gal}(F) := \text{Gal}(F^{\text{sep}}/F)$$

and call this group the *absolute Galois group* of the field F .

Since the field \mathbb{F}_p is perfect, we get that $\mathbb{F}_p^{\text{sep}} = \mathbb{F}_p^{\text{alg}}$ and $\text{Gal}(\mathbb{F}_p) = \text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p)$.

We consider now the *direct system* of finite Galois subextensions, where any such subextension is the following tower of fields:

$$K \subseteq K_i \subseteq M$$

and we assume that $K \subseteq K_i$ is a finite Galois extension.

Example 4.3. In the situation from the explicit example, we have:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^i} \subset \mathbb{F}_p^{\text{alg}}.$$

There is a set of indices I such that:

$$(K \subseteq K_i \subseteq M)_{i \in I}$$

is the collection of all such towers and we put a partial order on I by declaring:

$$i \leq j \quad \iff \quad K_i \subseteq K_j$$

(actually, this family of towers is “ordering itself” by inclusion, but it is aesthetically nicer to have this indexing partially ordered set I).

Example 4.4. In the situation from the explicit example, we have $I = \mathbb{N}_{>0}$. However, the order is not the usual order on $\mathbb{N}_{>0}$ but it is the *divisibility* order, since for $i, j \in \mathbb{N}_{>0}$, we have:

$$\mathbb{F}_{p^i} \subseteq \mathbb{F}_{p^j} \quad \iff \quad i|j.$$

Then, the collection:

$$(\mathrm{Gal}(K_i/K))_{i \in I}$$

becomes an *inverse system* of finite groups, that is for any $i \leq j$ we have the restriction group homomorphism

$$\mathrm{res}_i^j : \mathrm{Gal}(K_j/K) \longrightarrow \mathrm{Gal}(K_i/K), \quad \mathrm{res}_i^j(f) := f|_{K_i},$$

which (by finite Galois theory) is an epimorphism; and, moreover, for any $i \leq j \leq k$, we have the following:

$$(1) \quad \mathrm{res}_i^j \circ \mathrm{res}_j^k = \mathrm{res}_i^k, \quad \mathrm{res}_i^i = \mathrm{id}.$$

A general definition of an inverse system (of groups) is given below.

Definition 4.5. An *inverse system of groups* is a collection of groups $(G_i)_{i \in I}$ indexed by a partially ordered set (I, \leq) together with a collection of group homomorphisms

$$\left(r_i^j : G_j \longrightarrow G_i \right)_{i \leq j},$$

which satisfy Equation (1) above (for “ r ” in place of “ res ”).

For any $i \in I$, we also have the “big” restriction epimorphism:

$$\mathrm{res}_i : \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(K_i/K)$$

and for all $i \leq j$, the following holds:

$$(2) \quad \mathrm{res}_i^j \circ \mathrm{res}_j = \mathrm{res}_i.$$

The following commutative diagram may help to visualise this situation:

$$\begin{array}{ccc} & \mathrm{Gal}(M/K) & \\ \mathrm{res}_j \swarrow & & \searrow \mathrm{res}_i \\ \mathrm{Gal}(K_j/K) & \xrightarrow{\mathrm{res}_i^j} & \mathrm{Gal}(K_i/K). \end{array}$$

Example 4.6. In the situation from the explicit example, we have

$$\mathrm{Gal}(\mathbb{F}_{p^i}/\mathbb{F}_p) \cong C_i$$

(so, the prime number p “vanishes” from the picture). Moreover, each of the cyclic group $\mathrm{Gal}(\mathbb{F}_{p^i}/\mathbb{F}_p)$ comes with a particular choice of a generator, which is the Frobenius automorphism on \mathbb{F}_{p^i} . Let σ_i be the corresponding generator of C_i . If $i|j$, then the association $\sigma_j \mapsto \sigma_i$ uniquely extends to a group homomorphism $r_i^j : C_j \rightarrow C_i$ which corresponds to the restriction homomorphism:

$$\mathrm{res}_i^j : \mathrm{Gal}(\mathbb{F}_{p^j}/\mathbb{F}_p) \longrightarrow \mathrm{Gal}(\mathbb{F}_{p^i}/\mathbb{F}_p),$$

so $(C_i, r_i^j)_{i|j}$ is an inverse system of all finite cyclic groups.

The crucial thing here is the following universal property (Problem 4.1) saying that $\mathrm{Gal}(M/K)$ is the *inverse limit* (the formal definition follows the statement of the theorem) of the inverse system of groups $(\mathrm{Gal}(K_i/K))_{i \in I}$.

Theorem 4.7. *Suppose that H is a group and we also have a collection of homomorphisms $t_i : H \rightarrow \text{Gal}(K_i/K)$ such that for all $i \leq j$:*

$$\text{res}_i^j \circ t_j = t_i.$$

Then, there is a unique group homomorphism $\varphi : H \rightarrow \text{Gal}(M/K)$ such that for all $i \in I$ we have:

$$\text{res}_i \circ \varphi = t_i.$$

Definition 4.8. Let $(G_i, r_i^j)_{i,j \in I}$ be an inverse system of groups. An *inverse limit* of this inverse system is a group G together with a collection of group homomorphisms

$$(r_i : G \longrightarrow G_i)_{i \in I}$$

such that we have the following.

- (1) Equation (2) above holds (for “ r ” in place of “ res ”).
- (2) If H is a group together with a collection of homomorphisms $t_i : H \rightarrow G_i$ such that for all $i \leq j$, we have:

$$r_i^j \circ t_j = t_i;$$

then there is a unique group homomorphism $\varphi : H \rightarrow G$ such that for all $i \in I$ we have:

$$r_i \circ \varphi = t_i.$$

We usually express the fact that G is an inverse limit of the inverse system $(G_i)_{i \in I}$ (as you can see, we often skip r_i^j from the notation) by writing:

$$G = \varprojlim_{i \in I} G_i.$$

Example 4.9. In the situation from the explicit example, the inverse limit of the inverse system $(C_i)_{i \in \mathbb{N}_{>0}}$ from Example 4.6 coincides with the *profinite completion* of the additive group \mathbb{Z} , which is denoted by $\widehat{\mathbb{Z}}$. We will discuss profinite completions in general later.

Theorem 4.7 implies that the group $\text{Gal}(M/K)$ is fully determined by the inverse system of groups $(\text{Gal}(K_i/K))_i$. It can be explicitly formulated as follows (a more general version is stated in Theorem 4.11).

Theorem 4.10. *We define:*

$$\mathcal{G} := \left\{ (g_i)_{i \in I} \in \prod_{i \in I} \text{Gal}(K_i/K) \mid (\forall i \leq j) \left(\text{res}_i^j(g_j) = g_i \right) \right\}.$$

Then, we have the following:

- (1) \mathcal{G} is a subgroup of the group $\prod_{i \in I} \text{Gal}(K_i/K)$;
- (2) the map:

$$\text{Gal}(M/K) \longrightarrow \mathcal{G}, \quad f \mapsto (\text{res}_i(f))_{i \in I}$$

is an isomorphism of groups.

The pure group structure of $\text{Gal}(M/K)$ is not enough to yield a meaningful Galois theory. We also need a *topology* on $\text{Gal}(M/K)$, which comes from its description as the inverse limit of the inverse system $(\text{Gal}(K_i/K))_{i \in I}$. We recall some notions from point-set topology. If $(T_i)_{i \in I}$ is a collection of topological spaces, then the Cartesian product $\prod_{i \in I} T_i$ has a natural *Tychonoff topology*. The *Tychonoff Theorem* says that if all the T_i 's are compact Hausdorff, then the product $\prod_{i \in I} T_i$ is compact Hausdorff as well. We regard finite groups $\text{Gal}(K_i/K)$ as topological spaces with the discrete topology (any subset is open). Then, they are also compact Hausdorff and by Tychonoff Theorem, the product $\prod_{i \in I} \text{Gal}(K_i/K)$ is compact Hausdorff as well (but it is far from being discrete!).

We consider $\text{Gal}(M/K)$ as a topological space with the subspace topology induced from $\prod_{i \in I} \text{Gal}(K_i/K)$ (we identify $\text{Gal}(M/K)$ with \mathcal{G} using Theorem 4.10). For a description of the topological structure on $\text{Gal}(M/K)$, the following result is crucial, which we state in a more general context.

Theorem 4.11. *Let $(G_i, r_i^j)_{i,j \in I}$ be an inverse system of groups. We define:*

$$\mathcal{G} := \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i \mid (\forall i \leq j) (r_i^j(g_j) = g_i) \right\}.$$

We have the following:

- (1) \mathcal{G} is a subgroup of the group $\prod_{i \in I} G_i$;
- (2) \mathcal{G} (with the projection maps) is an inverse limit of the inverse system $(G_i, r_i^j)_{i,j \in I}$;
- (3) \mathcal{G} is a closed subset of the topological space $\prod_{i \in I} G_i$, where the G_i 's are considered with the discrete topology.

Proof. Item (1) is clear. Item (2) is Problem 4.2. Item (3) is (a special case of) Problem 4.3. □

Corollary 4.12. *$\text{Gal}(M/K)$ is a compact Hausdorff topological space.*

Proof. It follows from Theorem 4.11, since a finite discrete topological space is compact, and a closed subset of a compact Hausdorff space is again compact Hausdorff. □

The following general notion is strongly related to the topic we are discussing here.

Definition 4.13. A *topological group* is a pair (\mathcal{H}, \cdot) , where \mathcal{H} is a topological space and (\mathcal{H}, \cdot) is a group such that:

- (1) the group operation map:

$$\cdot : \mathcal{H} \times \mathcal{H} \longrightarrow \mathcal{H}$$

is continuous;

- (2) the inverse map:

$$^{-1} : \mathcal{H} \longrightarrow \mathcal{H}$$

is continuous.

It can be checked that $\text{Gal}(M/K)$ with the topology defined above is a topological group. Such topological groups are called *profinite*, the general definition is below.

Definition 4.14. A topological group \mathcal{H} is *profinite*, if it is isomorphic (as a topological group) to an inverse limit of finite groups with the topology from Theorem 4.11.

We present below a construction producing a profinite group from an arbitrary group.

Definition 4.15. Let H be an arbitrary group and $(H_i \triangleleft H)_{i \in I}$ be the direct system of all normal subgroups of H such that the index $[H : H_i]$ is finite. Then $(H/H_i)_{i \in I}$ is the inverse system of finite quotient groups of H . We define the *profinite completion* of H as:

$$\widehat{H} := \varprojlim_{i \in I} H/H_i.$$

Then, \widehat{H} is a profinite group. By the universal property of the inverse limit, the collection of quotient maps $(\pi_i : H \rightarrow H/H_i)_{i \in I}$ induces a unique (completion) homomorphism $\varphi : H \rightarrow \widehat{H}$ such that for any $i \in I$ the following diagram commutes:

$$\begin{array}{ccc} H & \xrightarrow{\varphi} & \widehat{H} \\ & \searrow \pi_i & \swarrow t_i \\ & H/H_i & \end{array}$$

By Problem 4.5(i), the image $\varphi(H)$ is dense in \widehat{H} (with the profinite topology). We give below some examples of profinite completions.

Example 4.16. Let H be a group.

- (1) If H is finite, then the natural map $H \rightarrow \widehat{H}$ is an isomorphism.
- (2) If $H = \mathbb{Z}$, then $(H/H_i)_{i \in I}$ from Definition 4.15 is an inverse system, which is isomorphic to the inverse system $(C_i)_{i \in \mathbb{N}_{>0}}$ from Example 4.6. By Problem 4.4, we get the following isomorphism of topological groups:

$$\text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}.$$

It can be shown (Problem 4.6) that:

$$\widehat{\mathbb{Z}} \cong \prod_{q \in \mathbb{P}} \mathbb{Z}_q,$$

where for each prime q , we have (the usual ordering on \mathbb{N}):

$$\mathbb{Z}_q := \varprojlim_{n \in \mathbb{N}} C_{q^n}.$$

It can be also shown that $\widehat{\mathbb{Z}}_q$ coincides with the additive group of the *ring of q -adic integers* (details may be given later in the lecture depending on time).

- (3) The profinite completion may be trivial, for example $\widehat{\mathbb{Q}} = \{0\}$ (the same holds for an arbitrary divisible commutative group). Obviously, in such a case the map $\mathbb{Q} \rightarrow \widehat{\mathbb{Q}}$ is the 0-map, in particular it is not injective. By Problem 4.5(ii), we have in general that:

$$\ker(\varphi : H \rightarrow \widehat{H}) = \bigcap_{i \in I} H_i$$

(H_i 's above are normal subgroups of H of finite index).

We are ready now to state the fundamental theorem of infinite Galois theory. We will skip the proof (except the closed subgroup condition: Problem 4.7).

Theorem 4.17. *Assume that $K \subseteq M$ is a Galois extension (possibly infinite) and we consider $\text{Gal}(M/K)$ as a profinite topological group. We have the following.*

(1) *The association:*

$$F \mapsto \text{Gal}(M/F)$$

gives a bijection between the family of towers of fields $K \subseteq F \subseteq M$ and the family of closed subgroups of $\text{Gal}(M/K)$.

(2) *The inverse map to the map from Item (1) is given by:*

$$H \mapsto M^H.$$

(3) *The above maps reverse inclusions and we have:*

$$[F : K] = [\text{Gal}(M/K) : \text{Gal}(M/F)].$$

(4) *The field extension $K \subseteq F$ is Galois if and only if $\text{Gal}(M/F) \triangleleft \text{Gal}(M/K)$. In such a case, we have the following:*

$$\text{Gal}(F/K) \cong \text{Gal}(M/K) / \text{Gal}(M/F).$$

Example 4.18. For the Galois extension $\mathbb{F}_p \subset \mathbb{F}_p^{\text{alg}}$, we know that:

$$\text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p) \cong \widehat{\mathbb{Z}} \cong \prod_{q \in \mathbb{P}} \mathbb{Z}_q.$$

The finite extensions $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ correspond to the closed subgroups of finite index in $\widehat{\mathbb{Z}}$ (actually, *any* subgroup of finite index in $\widehat{\mathbb{Z}}$ is closed), which further correspond to finite index subgroups $n\mathbb{Z}$ in \mathbb{Z} (since $\widehat{\widehat{\mathbb{Z}}} = \widehat{\mathbb{Z}}$). We also have the following:

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p) / \text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_{p^n}) \cong \widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z} \cong C_n.$$

To give an example of an infinite extension, let us fix $r \in \mathbb{P}$ and consider:

$$\mathcal{H} := \prod_{q \in \mathbb{P} \setminus \{r\}} \mathbb{Z}_q < \widehat{\mathbb{Z}}.$$

Then, we have:

$$\left(\mathbb{F}_p^{\text{alg}}\right)^{\mathcal{H}} = \left(\bigcup_{n>0} \mathbb{F}_{p^n}\right)^{\mathcal{H}} = \bigcup_{i>0} \mathbb{F}_{r^q i}$$

(note that the first infinite union is not increasing and that the second infinite union is increasing).

The closed condition is crucial in Theorem 4.17 as the following example shows.

Example 4.19. Since $\bigcap_n n\mathbb{Z} = \{0\}$, Problem 4.5(ii) implies that the completion map $\varphi : \mathbb{Z} \rightarrow \widehat{\mathbb{Z}}$ is one-to-one. Hence, we consider \mathbb{Z} as a subgroup of $\widehat{\mathbb{Z}} = \text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p)$. By Problem 4.5(i), \mathbb{Z} is dense in $\widehat{\mathbb{Z}}$. In particular, \mathbb{Z} is not a closed subgroup of $\widehat{\mathbb{Z}}$ (it is easy to see, for instance by Example 4.18, that $\mathbb{Z} \neq \widehat{\mathbb{Z}}$). Therefore, \mathbb{Z} does not correspond to any subfield of $\mathbb{F}_p^{\text{alg}}$.

Problem List 4

- (1) We assume that $K \subseteq M$ is a Galois extension and $(K \subseteq K_i \subseteq M)_{i \in I}$ is the collection of all towers of fields such that $K \subseteq K_i$ is a finite Galois extension.
- (a) Let $g, g' \in \text{Gal}(M/K)$ be such that for all $i \in I$, we have $g|_{K_i} = g'|_{K_i}$. Show that $g = g'$.
- (b) Let $(g_i \in \text{Gal}(K_i/K))_{i \in I}$ be such that for all $i \leq j$ we have $g_j|_{K_i} = g_i$. Show that there is $g \in \text{Gal}(M/K)$ such that for all $i \in I$ we have $g|_{K_i} = g_i$.
- (c) Show that:

$$\text{Gal}(M/K) = \varprojlim_{i \in I} \text{Gal}(K_i/K).$$

- (2) Let $(G_i, r_i^j)_{i, j \in I}$ be an inverse system of groups. We define:

$$\mathcal{G} := \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i \mid (\forall i \leq j) (r_i^j(g_j) = g_i) \right\}.$$

Show that \mathcal{G} (with the projection maps) is an inverse limit of the inverse system $(G_i, r_i^j)_{i, j \in I}$.

- (3) Suppose that $(T_i, r_i^j)_{i, j \in I}$ is an *inverse system of topological spaces* (the same definition as for groups after replacing “homomorphism” with “continuous map”). We define:

$$\mathcal{T} := \left\{ (x_i)_{i \in I} \in \prod_{i \in I} T_i \mid (\forall i \leq j) (r_i^j(x_j) = x_i) \right\}.$$

Assume moreover that all the topological spaces T_i are Hausdorff. Show that \mathcal{T} is a closed subset of the topological space $\prod_{i \in I} T_i$.

- (4) Show that:

$$\widehat{\mathbb{Z}} = \varinjlim_{n \in \mathbb{N}_{>0}} C_n,$$

where the inverse system $(C_i, r_i^j)_{i, j}$ was described in Example 4.6 (it is enough to know that all the maps r_i^j are onto).

- (5) Let H be an arbitrary group and $\varphi : H \rightarrow \widehat{H}$ be the completion homomorphism. Show the following.

- (a) The set $\varphi(H)$ is dense in \widehat{H} (with the profinite topology).
- (b) We have:

$$\ker(\varphi : H \rightarrow \widehat{H}) = \bigcap_{i \in I} H_i$$

(H_i 's above are normal subgroups of H of finite index).

- (6) Show that:

$$\widehat{\mathbb{Z}} \cong \prod_{q \in \mathbb{P}} \mathbb{Z}_q,$$

where for each prime q , we have (with the usual ordering on \mathbb{N}):

$$\mathbb{Z}_q := \varprojlim_{n \in \mathbb{N}} C_{q^n}.$$

- (7) Let $K \subseteq F \subseteq M$ be a tower of fields such that the extension $K \subseteq M$ is Galois. Show that $\text{Gal}(M/F)$ is a closed subset of $\text{Gal}(M/K)$.

5. FRATTINI COVERS AND EXISTENTIALLY CLOSED G -FIELDS

In today's lecture, we start from a more detailed analysis of Example 4.18. Then, we describe Galois-theoretically a property of G -fields which is responsible for a "half" of the existential closedness.

5.1. Galois correspondence for the absolute Galois group of \mathbb{F}_p . In this part, we study more closely Example 4.18 regarding the Galois correspondence related to the field extension $\mathbb{F}_p \subset \mathbb{F}_p^{\text{alg}}$. We need an explicit description of the isomorphism $\text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}$. This description will also clarify some issues from Example 4.19.

It follows from the definitions that there is the following commutative diagram:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \widehat{\mathbb{Z}} \\ & \searrow \alpha & \uparrow \psi \\ & & \text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p), \end{array}$$

where:

- the homomorphism φ is the profinite completion map;
- the homomorphism ψ is the map given by the universal property of the inverse limit and the following collection of maps:

$$\left(\widetilde{\text{res}}_n : \text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p) \longrightarrow \mathbb{Z}/n\mathbb{Z} \right)_{n>0},$$

where each $\widetilde{\text{res}}_n$ is given by the following composition:

$$\text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p) \xrightarrow{\text{res}_n} \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \xrightarrow{\cong} \mathbb{Z}/n\mathbb{Z},$$

where the last isomorphism maps the Frobenius map on \mathbb{F}_{p^n} to $1 + n\mathbb{Z}$;

- the homomorphism α is such that $\alpha(1)$ is the Frobenius map on $\mathbb{F}_p^{\text{alg}}$.

We recall the isomorphism

$$\widehat{\mathbb{Z}} \cong \prod_{q \in \mathbb{P}} \mathbb{Z}_q$$

from Problem 4.6. Let us fix $n > 0$. We want to understand the restriction map

$$\text{res}_n : \text{Gal}(\mathbb{F}_p^{\text{alg}}/\mathbb{F}_p) \longrightarrow \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$$

as a map

$$\prod_{q \in \mathbb{P}} \mathbb{Z}_q \longrightarrow C_n.$$

Let

$$n = \prod_{q \in \mathbb{P}} q^{v_q}, \quad C_n \cong \prod_{q \in \mathbb{P}} C_{q^{v_q}}$$

be the decomposition of the number n as a product of powers of pairwise distinct primes, and we also note the corresponding decomposition of the cyclic group C_n (Chinese Remainder Theorem). These products look infinite, but they are in fact finite, since almost all v_q (the q -adic valuations applied to n) are 0. We have the corresponding two epimorphisms:

$$r_{q,v_q} : \mathbb{Z}_q \longrightarrow C_{q^{v_q}}, \quad r_{n,q} : C_n \longrightarrow C_{q^{v_q}}.$$

We have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{F}_p^{\mathrm{alg}}/\mathbb{F}_p) & \xrightarrow{\mathrm{res}_n} & \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \\ \cong \downarrow \Psi & & \cong \downarrow \\ \prod_q \mathbb{Z}_q & \xrightarrow{\prod_q r_q, v_q} & \prod_q C_{q^{v_q}}, \end{array}$$

where the isomorphism Ψ is given by the following three things:

- the universal property of the inverse limit;
- the universal property of the product;
- for each $q \in \mathbb{P}$, the following collection of maps:

$$\left(\widetilde{\mathrm{res}}_{q^i} : \mathrm{Gal}(\mathbb{F}_p^{\mathrm{alg}}/\mathbb{F}_p) \longrightarrow C_{q^i} \right)_i,$$

where the homomorphisms $\widetilde{\mathrm{res}}_{q^i}$ were defined above.

Problem 5.1 says that in the general setting of an arbitrary Galois extension $K \subseteq M$, if $\mathcal{H} \leq \mathrm{Gal}(M/K)$ and for each $i \in I$ we define:

$$H_i := \mathrm{res}_i(\mathcal{H}) \leq \mathrm{Gal}(K_i/K),$$

then we have $M = \bigcup_i K_i$, and we also obtain:

$$M^{\mathcal{H}} = \left(\bigcup_i K_i \right)^{\mathcal{H}} = \bigcup_i (K_i)^{H_i}.$$

Finally, we apply all the above to the case of

$$\mathcal{H} := \prod_{q \in \mathbb{P} \setminus \{r\}} \mathbb{Z}_q < \widehat{\mathbb{Z}} = \mathrm{Gal}(\mathbb{F}_p^{\mathrm{alg}}/\mathbb{F}_p)$$

from Example 4.18. Using the commutative diagram above, we have the following description of the groups H_n , which were introduced in Problem 5.1:

$$H_n := \mathrm{res}_n(\mathcal{H}) = C_{n_r} \leq C_n = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p),$$

where the number n_r is defined as:

$$n_r := \prod_{q \neq r} q^{n_q} = \frac{n}{r^{v_r}},$$

and we identify C_{n_r} with a unique cyclic subgroup of order n_r in C_n . We obtain the following (we use below “ $v_r(n)$ ” instead of “ v_r ” to emphasize the dependence on n):

$$\begin{aligned} (\mathbb{F}_p^{\text{alg}})^{\mathcal{H}} &= \left(\bigcup_n \mathbb{F}_{p^n} \right)^{\mathcal{H}} \\ &= \bigcup_n (\mathbb{F}_{p^n})^{H_n} \\ &= \bigcup_n (\mathbb{F}_{p^n})^{C_{n_r}} \\ &= \bigcup_n \mathbb{F}_{p^{r v_r(n)}} \\ &= \bigcup_i \mathbb{F}_{p^{r^i}} \end{aligned}$$

as claimed in Example 4.18. If we denote:

$$\mathbb{F}_{p^{q^\infty}} := \bigcup_i \mathbb{F}_{p^{q^i}},$$

then we have the equality (Problem 5.2):

$$\mathbb{F}_p^{\text{alg}} = \prod_{q \in \mathbb{P}} \mathbb{F}_{p^{q^\infty}},$$

where the product on the right-hand-side stands for the (infinite) *compositum* of subfields of $\mathbb{F}_p^{\text{alg}}$. This last equality corresponds to the isomorphism:

$$\widehat{\mathbb{Z}} \cong \prod_{q \in \mathbb{P}} \mathbb{Z}_q.$$

5.2. G -closed fields and Frattini covers. We come back to our situation of interest. Let G be a finite non-trivial group. We want to understand e.c. G -fields. The material here comes from:

[HK] Daniel Hoffmann, Piotr Kowalski “Existentially closed fields with finite group actions”, *Journal of Mathematical Logic*, (1) 18 (2018), 1850003.

However, many results from [HK] had been also obtained independently by Sjögren 10 years earlier, the related story can be found in [HK].

Let us fix a G field K . We do not notationally differentiate between a G -field and its underlying field (and its underlying universe). By Problem 3.7: if K is e.c., then K is perfect. Hence, it is natural to assume that K is perfect and we make this assumption. We introduce one more property below (it makes sense for an arbitrary group G).

Definition 5.1. A G -field K is *strict*, if the action of G on K is faithful.

The result below is Problem 5.4.

Fact 5.2. (1) *The G -field K is strict if and only if:*

$$[K : K^G] = |G|.$$

- (2) If K is strict, then $G \cong \text{Gal}(K/K^G)$.
- (3) If $K \subseteq K'$ is a G -field extension and K is strict, then K' is also strict.

Problem 5.5 says that an e.c. G -field is strict. Therefore, we assume that K is strict and we make the following identification:

$$G = \text{Gal}(K/K^G).$$

It is also clear that an e.c. G -field does not have any proper algebraic (in the field sense) extensions. We specify such G -fields below.

Definition 5.3. A G -field is G -closed, if it has no proper algebraic (in the field sense) extensions.

All these particular properties of e.c. G -fields mentioned above (perfectness, strictness, and G -closedness) are not enough to guarantee the existential closedness as the following example shows.

Example 5.4. We consider (\mathbb{C}, σ) as a C_2 -field, where σ is the complex conjugation. This C_2 -field is clearly perfect, strict, and C_2 -closed (since \mathbb{C} is even algebraically closed). However, by Example 3.5, the C_2 -field (\mathbb{C}, σ) is not existentially closed.

There is one more condition of a geometric nature which (together with the previous ones) *implies* the existential closedness. We will discuss it next week. At this moment, we present the Galois-theoretic condition which is equivalent to the G -closedness condition.

Recall that K is a perfect and strict G -field. We set $C := K^G$ and we identify G with $\text{Gal}(K/C)$. By Problem 3.2, C is a perfect field as well. Let us set:

$$\mathcal{G} := \text{Gal}(C) = \text{Gal}(C^{\text{alg}}/C).$$

Then, we have the restriction map:

$$\text{res} : \mathcal{G} \longrightarrow G = \text{Gal}(K/C)$$

and we define:

$$\mathcal{N} := \ker(\text{res} : \mathcal{G} \longrightarrow G).$$

By the fundamental theorem of Galois theory, we have:

$$\mathcal{N} = \text{Gal}(C^{\text{alg}}/K)$$

and, obviously, we also have that $\mathcal{G}/\mathcal{N} \cong G$. We state now the main result of today's lecture.

Theorem 5.5 (Lemma 3.7 in [HK]). *The following are equivalent.*

- (1) *There is a proper algebraic G -field extension $K \subset K'$.*
- (2) *There is a proper closed subgroup $\mathcal{G}_0 < \mathcal{G}$ such that $\text{res}(\mathcal{G}_0) = G$.*

Proof. (1) \Rightarrow (2) Let us assume that $K \subset K'$ is a proper algebraic G -field extension. We define:

$$C' := (K')^G, \quad \mathcal{G}_0 := \text{Gal}(C') = \text{Gal}(C^{\text{alg}}/C').$$

By the fundamental theorem of Galois theory, \mathcal{G}_0 is a closed subgroup of \mathcal{G} . We need to show the following:

- (i) $\mathcal{G}_0 \neq \mathcal{G}$,
- (ii) $\text{res}(\mathcal{G}_0) = G$.

Let us consider first the following restriction homomorphism (it is well-defined, since the extension $C \subset K$ is Galois):

$$\text{res}_K^{K'} : \text{Gal}(K'/C) \longrightarrow \text{Gal}(K/C) = G.$$

By Fact 5.2(iii), K' is strict, so (by Fact 5.2(ii)) $\text{Gal}(K'/C') \cong G$. Since $K \subset K'$ is a G -field extension, we get that:

$$(*) \quad \text{res}_K^{K'}(\text{Gal}(K'/C')) = G,$$

so the map $\text{res}_K^{K'}$ restricted to $\text{Gal}(K'/C')$ is an isomorphism.

We have the following commutative diagram of field extensions:

$$\begin{array}{ccc} C' & \longrightarrow & K' \\ \uparrow & & \uparrow \\ C & \longrightarrow & K. \end{array}$$

Therefore, we get:

$$[K' : C'][C' : C] = [K' : K][K : C].$$

Since we have (see Fact 5.2(i)):

$$[K' : C'] = |G| = [K : C],$$

we get that:

$$[C' : C] = [K' : K] > 1,$$

since the extension $K \subset K'$ is proper. Therefore, the extension $C \subset C'$ is proper as well. By the fundamental theorem of Galois theory, we get $\mathcal{G}_0 \neq \mathcal{G}$ showing Item (i).

To show Item (ii), we consider the following commutative diagram of groups:

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\text{res}} & G \\ \uparrow & & \uparrow \text{res}_K^{K'} \\ \mathcal{G}_0 & \xrightarrow{\text{res}|_{\mathcal{G}_0}} & \text{Gal}(K'/C'). \end{array}$$

Using this diagram, the fact that the map $\text{res}|_{\mathcal{G}_0}$ is onto (since the field extension $C' \subseteq K'$ is Galois), and Equation (*); we get that $\text{res}(\mathcal{G}_0) = G$ showing Item (ii).

(2) \Rightarrow (1) Let \mathcal{G}_0 be a proper closed subgroup of \mathcal{G} such that $\text{res}(\mathcal{G}_0) = G$. Since $\text{res}(\mathcal{G}_0) = G$ and $\mathcal{N} = \ker(\text{res})$, we get that $\mathcal{N}\mathcal{G}_0 = \mathcal{G}$. We define:

$$C' := (C^{\text{alg}})^{\mathcal{G}_0}, \quad K' := (C^{\text{alg}})^{\mathcal{G}_0 \cap \mathcal{N}}.$$

Since we have:

$$\mathcal{G}_0 = \text{Gal}\left((C')^{\text{alg}}/C'\right), \quad \mathcal{G}_0 \cap \mathcal{N} = \text{Gal}\left((C')^{\text{alg}}/K'\right) \triangleleft \mathcal{G}_0,$$

by the fundamental theorem of Galois theory, the field extension $C' \subseteq K'$ is Galois and we have:

$$\begin{aligned} \text{Gal}(K'/C') &\cong \text{Gal}\left((C')^{\text{alg}}/C'\right) / \text{Gal}\left((C')^{\text{alg}}/K'\right) \\ &\cong \mathcal{G}_0 / (\mathcal{G}_0 \cap \mathcal{N}) \\ &\cong G, \end{aligned}$$

where the last isomorphism follows from $\text{res}(\mathcal{G}_0) = G$ and

$$\ker(\text{res}) \cap \mathcal{G}_0 = \mathcal{N} \cap \mathcal{G}_0.$$

We need to show the following:

- (i) K is a proper subfield of K' ,
- (ii) $K \subset K'$ has a structure of a G -field extension.

Since $\mathcal{N}\mathcal{G}_0 = \mathcal{G}$ and $\mathcal{G}_0 \neq \mathcal{G}$, we get that \mathcal{N} is *not* a subgroup of \mathcal{G}_0 . Therefore, we have:

$$\mathcal{G}_0 \cap \mathcal{N} \not\cong \mathcal{N},$$

so, by the Galois correspondence, we obtain:

$$K = \left(C^{\text{alg}}\right)^{\mathcal{N}} \subsetneq \left(C^{\text{alg}}\right)^{\mathcal{G}_0 \cap \mathcal{N}} = K'$$

showing Item (i).

To show Item (ii), we have to define an action of G on K' (by field automorphisms), which extends our fixed action of G on K . We consider the same restriction map as in the proof of the other implication:

$$\text{res}_K^{K'} : \text{Gal}(K'/C) \longrightarrow \text{Gal}(K/C) = G.$$

By the Galois correspondence, the intersection of subgroups corresponds to the compositum of subfields, therefore we get the following:

$$KC' = \left(C^{\text{alg}}\right)^{\mathcal{N}} \left(C^{\text{alg}}\right)^{\mathcal{G}_0} = \left(C^{\text{alg}}\right)^{\mathcal{N} \cap \mathcal{G}_0} = K'.$$

Since $KC' = K'$, the map:

$$\alpha := \left(\text{res}_K^{K'}\right) |_{\text{Gal}(K'/C')} : \text{Gal}(K'/C') \longrightarrow \text{Gal}(K/C) = G$$

is one-to-one. Since $\text{Gal}(K'/C') \cong G$ (a finite group), we get that the map α is an isomorphism. The fact that the restriction map induces the isomorphism:

$$\text{Gal}(K'/C') \cong \text{Gal}(K/C) = G$$

means that after defining the G -field structure on K' using this last isomorphism, the field extension $K \subset K'$ becomes a G -field extension giving Item (ii) and finishing the proof. \square

We need one notion from the theory of profinite groups, which naturally appeared in the statement of Theorem 5.5. Let \mathcal{H} and \mathcal{G} be profinite groups.

Definition 5.6. A continuous epimorphism $f : \mathcal{H} \rightarrow \mathcal{G}$ is a *Frattini cover*, if for any closed subgroup $\mathcal{H}_0 \leq \mathcal{H}$, we have that $f(\mathcal{H}_0) = \mathcal{G}$ if and only if $\mathcal{H}_0 = \mathcal{H}$.

Problem 5.6 gives examples and counterexamples for the notion of a Frattini cover.

We get the following obvious conclusion of Theorem 5.5, which is our Galois-theoretic characterization of G -closed G -fields.

Corollary 5.7. *The G -field K is G -closed if and only if the restriction map*

$$\text{res} : \text{Gal}(C) \longrightarrow \text{Gal}(K/C) = G$$

is a Frattini cover.

Problem List 5

Let p and q be prime numbers.

- (1) Let $K \subseteq M$ be a Galois extension and

$$(K \subseteq K_i \subseteq M)_{i \in I}$$

be the direct system of field towers such that $K \subseteq K_i$ is a finite Galois extensions. We fix $\mathcal{H} \leq \text{Gal}(M/K)$ and for each $i \in I$, we define:

$$H_i := \text{res}_i(\mathcal{H}) \leq \text{Gal}(K_i/K).$$

Show the following.

- (a) $M = \bigcup_{i \in I} K_i$.
 (b) We have:

$$M^{\mathcal{H}} = \bigcup_i (K_i)^{H_i}.$$

- (2) Let us denote:

$$\mathbb{F}_{p^{q^\infty}} := \bigcup_i \mathbb{F}_{p^{q^i}}.$$

Show the following equality:

$$\mathbb{F}_p^{\text{alg}} = \prod_{q \in \mathbb{P}} \mathbb{F}_{p^{q^\infty}},$$

where the product on the right-hand-side stands for the (infinite) compositum of subfields of $\mathbb{F}_p^{\text{alg}}$.

- (3) Show that the multiplicative groups \mathbb{C}^* , $(\mathbb{F}_p^{\text{alg}})^*$ are divisible, and find their corresponding decompositions from Problem 2.7(a).
 (4) Let K be a G -field, where G is a finite group. Show the following.
 (a) The following are equivalent.
 (i) The G -field K is strict.
 (ii) $[K : K^G] = |G|$.
 (iii) $G \cong \text{Gal}(K/K^G)$.
 (b) If $K \subseteq K'$ is a G -field extension and K is strict, then K' is also strict.
 (5) Let G be an arbitrary group and K be an existentially closed G -field. Show that K is strict.
 (6) (a) Show that the following epimorphisms

$$C_4 \longrightarrow C_2, \quad C_{p^n} \longrightarrow C_{p^m}, \quad \mathbb{Z}_p \longrightarrow C_{p^m}$$

are Frattini covers.

- (b) Find an example of an epimorphism of finite groups which is *not* a Frattini cover.

6. PAC FIELDS AND EXISTENTIALLY CLOSED G -FIELDS

In today's lecture, we introduce the notion of a *pseudo algebraically closed* (PAC) field. Then, we will see that the PAC property is responsible for the second “half” of the existential closedness of G -fields.

6.1. Pseudo algebraically closed fields. We know that if G is finite and non-trivial, then e.c. G fields are *not* algebraically closed. However, such (pure) fields should still be reasonably large in some other sense. In this part of the lecture, we specify and discuss this: “some other sense”.

We start with an observation. By Hilbert's Nullstellensatz, a field K is algebraically closed if and only if for all $n > 0$, all prime ideals in $K[X_1, \dots, X_n]$ have zeroes in K . In other words (recall the vocabulary from Section 1), for all K -irreducible K -varieties V , the set of *rational points* $V(K)$ should be non-empty. If we replace the K -irreducibility notion above with a stronger notion of the *absolute irreducibility*, then we get a weaker property of fields, which is exactly the PAC property being the topic of today's lecture. The formal definition is below.

Definition 6.1. A field K is *pseudo algebraically closed* (abbreviated PAC), if for any absolutely irreducible K -variety V , we have that $V(K) \neq \emptyset$.

It is easy to see that if V is a *plane curve*, that is $V = Z(F)$ for some $F \in K[X_1, X_2]$, then V is absolutely irreducible if and only if F is an irreducible element in the ring $K^{\text{alg}}[X_1, X_2]$. We call such polynomials “absolutely irreducible” as well.

Example 6.2. Similarly as with algebraically closed fields, it is not easy to give satisfactory examples of PAC fields (note that there is only one natural example of an algebraically closed field: the field of complex numbers!).

- (1) Obviously, each algebraically closed field is PAC.
- (2) Each separably closed field is PAC, which is more difficult to show.
- (3) We will see that \mathbb{R} is *not* PAC by looking at plane curves or at polynomials in two variables. Problem 6.5 says that the polynomial $X_1^2 + X_2^2 \in \mathbb{R}[X_1, X_2]$ is irreducible but it is not absolutely irreducible (a warm-up case), and that the polynomial $X_1^2 + X_2^2 + 1 \in \mathbb{R}[X_1, X_2]$ is absolutely irreducible. Since the polynomial $X_1^2 + X_2^2 + 1$ has no zeroes in \mathbb{R} , the field \mathbb{R} is not PAC.
- (4) Finite fields are not PAC (Example 11.2.9 in [FJ], see below), but are “closer and closer” to being PAC (see Theorem 6.7). This implies (together with Theorem 6.3) that non-principal ultraproducts of finite fields *are* PAC. We will comment more about it while discussing Ax's theorem (Theorem 6.14) below.

We need to use several results about PAC fields and we do not have time to present their proofs. Not all of them are necessary for the proof of the main result of today's lecture (Corollary 6.20), but they give a better understanding of the PAC notion. The full proofs of these results would probably need another one-semester lecture whose title could be “Field Arithmetic”, which is also the title of the following book where those proofs can be found:

[FJ] M.D. Fried, M. Jarden, “Field Arithmetic”, 3rd Edition, Springer.

Theorem 6.3 (Proposition 11.3.2 in [FJ]). *The PAC property is first-order, that is there is a theory T in the language of rings such that models of T are exactly PAC fields.*

Problem 6.1 says that for a field extension $K \subseteq M$, we have the following:

- (1) there is a continuous homomorphism:

$$\text{res} : \text{Gal}(M) \longrightarrow \text{Gal}(K), \quad \text{res}(f) = f|_{K^{\text{alg}}};$$

- (2) if $K \preceq M$, then the map $\text{res} : \text{Gal}(M) \rightarrow \text{Gal}(K)$ is an epimorphism.

The next theorem gives a version of a converse statement (to the implication from Problem 6.1(2)) for PAC fields, which is crucial for our proof of Theorem 6.19. This result is stated in a more general and also more complicated way in [FJ].

Theorem 6.4 (Corollary 20.3.4 in [FJ]). *If $K \subseteq M$ is an extension of perfect PAC fields and the restriction map $\text{res} : \text{Gal}(M) \longrightarrow \text{Gal}(K)$ is an isomorphism, then $K \preceq M$.*

The next two results provide some information about algebraic extensions and the PAC property.

Theorem 6.5 (Ax-Roquette, Corollary 11.2.5 in [FJ]). *An algebraic extension of a PAC field is again PAC.*

Theorem 6.6 (Ershov, Corollary 11.2.4 in [FJ]). *An infinite algebraic extension of a finite field is PAC.*

The result below should be understood as saying that if we look at larger and larger finite fields, then they become “more and more PAC”.

Theorem 6.7 (special case of *Lang-Weil estimates*, Theorem 5.4.1 in [FJ]). *Let q be a power of a prime number and $F \in \mathbb{F}_q[X_1, X_2]$ be an absolutely irreducible polynomial of the total degree d . If we set $\Gamma := Z(F)$, then we have:*

$$q + 1 - (d - 1)(d - 2)\sqrt{q} - d \leq |\Gamma(\mathbb{F}_q)| \leq q + 1 + (d - 1)(d - 2)\sqrt{q}.$$

A similar result holds for arbitrary absolutely irreducible \mathbb{F}_q -varieties.

Before the next and final result about PAC fields (which is also crucial for us), we need one more definition.

Definition 6.8. A profinite group \mathcal{G} is *projective*, if for every continuous epimorphism of profinite groups $\alpha : \mathcal{H} \rightarrow \mathcal{G}$ there is a section $\beta : \mathcal{G} \rightarrow \mathcal{H}$, that is $\alpha \circ \beta = \text{id}_{\mathcal{G}}$.

Remark 6.9. The notion of a projective profinite group is analogous to the notion of a projective module. Similarly as in the case of modules, *free profinite* groups are projective. We will not give a definition of the notion of “free profinite” here, but, for example, $\widehat{\mathbb{Z}}$ is a free profinite group on one generator.

Theorem 6.10 (Theorem 11.6.2 in [FJ]). *If K is a PAC field, then the absolute Galois group $\text{Gal}(K)$ is projective.*

Remark 6.11. The opposite implication does not hold. For example, a finite field is not PAC, but its absolute Galois group (which is $\widehat{\mathbb{Z}}$) is projective.

We will discuss now one more notion which we do not need for any proofs, but it is naturally related to the main topic. Let us define the *theory of finite fields* as:

$$T_{\text{ff}} := \bigcap_{p \in \mathbb{P}} \bigcap_{n=1}^{\infty} \text{Th}(\mathbb{F}_{p^n}).$$

The theory T_{ff} consists of those sentences in the language of rings which are true in *all* finite fields. In particular, any finite field is a model of T_{ff} .

Example 6.12. We will see examples of two sentences from the theory of finite fields.

- (1) Let $p \in \mathbb{P}$ and φ_p be the following sentence in the language of rings:

$$\underbrace{1 + \dots + 1}_{p \text{ times}} = 0 \quad \Rightarrow \quad \forall x \exists y \ x = y^p.$$

Then, for all $p \in \mathbb{P}$, we have $\varphi_p \in T_{\text{ff}}$. Therefore, models of T_{ff} are perfect fields (but, of course, not all perfect fields are models of T_{ff}).

- (2) For any $n > 0$, let ψ_n be a sentence in the language of rings expressing that all field extensions of degree n are Galois and cyclic (such a sentence exists). Then, we have $\psi_n \in T_{\text{ff}}$.

Definition 6.13. A field K is *pseudofinite*, if it is an infinite model of the theory T_{ff} .

A similar notion can be defined for an arbitrary theory in place of the theory of fields, yielding a notion of a *pseudofinite model* of a given theory. For instance a pseudofinite set (that is: a pseudofinite model of the empty theory in the language of equality) is the same as an infinite set, which may be a slightly confusing example. Problem 6.6(b) says that a field is pseudofinite if and only if it is elementarily equivalent to a non-principal ultraproduct of finite fields.

It is usually not easy to *characterize* pseudofinite models (for example: pseudofinite groups are rather mysterious, see Problem 6.6(c,d)). However, in the case of fields it was done by James Ax.

Theorem 6.14 (Ax, Corollary 20.10.5 in [FJ]). *Let K be a field. Then, K is pseudofinite if and only if the following holds:*

- (1) K is perfect;
- (2) K is PAC;
- (3) for each $n > 0$, K has a unique algebraic extension of degree n (inside a fixed algebraic closure K^{alg}).

Remark 6.15. More comments on Ax's theorem and pseudofinite fields are below.

- By Example 6.12(1), pseudofinite fields are perfect. By Theorem 6.3, Theorem 6.7, and Problem 6.6(b), finite fields are “PAC enough” to guarantee that pseudofinite fields are PAC. By Problem 6.8, the uniqueness property from Item (3) above is first-order as well and since finite fields have it, pseudofinite fields have it as well. The difficult part of the proof of Ax's Theorem is the opposite implication and we do not have time to discuss it.
- Item (3) in Ax's Theorem is equivalent to saying that $\text{Gal}(K) \cong \widehat{\mathbb{Z}}$.
- Algebraically closed fields are *not* pseudofinite. Problem 6.4 is about finding a subfield of $\mathbb{F}_p^{\text{alg}}$ which is pseudofinite.

6.2. Galois-theoretic description of e.c. G -fields. We have all the ingredients now to show that the theory of G -fields has a model companion and to give axioms of this model companion in a *Galois-theoretic* way. Next week, we will discuss *geometric* axioms of this model companion. Firstly, we isolate the last missing property of e.c. G -fields (G finite).

Theorem 6.16. *If K is an e.c. G -field and $C := K^G$, then the field C is PAC.*

Proof. We present here the proof of Sjögren. Let V be an absolutely irreducible C -variety, where K is an e.c. G -field and $C := K^G$. It means that $V = Z(I)$ for some $I \trianglelefteq C[X]$ such that I is prime and the ideal $IC^{\text{alg}}[X]$ is prime in the ring $C^{\text{alg}}[X]$. Then, the ideal

$$I_K := IK[X] \trianglelefteq K[X]$$

is prime as well, which is all we will need (so, we will not use the fact that C is “fully PAC”).

Let us define the following *coordinate rings*:

$$C[V] := C[X]/I, \quad K[V] := C[V] \otimes_C K.$$

We use a basic fact about tensor products of algebras for the isomorphism below:

$$\begin{aligned} K[V] &= C[V] \otimes_C K \\ &= (C[X]/I) \otimes_C K \\ &\cong K[X]/(IK[X]) \\ &= K[X]/I_K. \end{aligned}$$

Since the ideal I_K is prime, $K[V]$ is a domain. Let $K(V)$ (the field of *rational functions*) denote the field of fractions of $K[V]$.

We aim to show that the field extension $K \subset K(V)$ has a G -field extension structure. By Problem 6.7, $K \subset C[V] \otimes_C K$ has a natural G -ring extension structure such that the action of G on $C[V]$ is trivial. By Problem 6.8, $K \subset K(V)$ has a natural structure of a G -field extension indeed. As usual, we have $(X = (X_1, \dots, X_n))$:

$$(X_1 + I_K, \dots, X_n + I_K) \in V(K(V)).$$

By the construction of the G -field structure on $K(V)$, we get that:

$$(X_1 + I_K, \dots, X_n + I_K) \in V((K(V))^G).$$

Since the field of G -invariants is definable (using that the group G is finite) and K is an e.c. G -field, we get that $V(C) \neq \emptyset$, which we needed to show. \square

Remark 6.17. (1) Since the extension $C \subseteq K$ is algebraic and C is PAC, we get that K is PAC by Theorem 6.5.

- (2) There is a direct argument (using the notion of a *regular field extension*) showing that for an *arbitrary* group G and an e.c. closed G -field K , K is PAC.
- (3) The argument above showing that if K is an e.c. G -field, then K^G is PAC works for finitely generated groups G as well.
- (4) It is not clear whether for an arbitrary group G and an e.c. G -field K , K^G is PAC. The problem is that K^G need not be definable in general (it is merely *type-definable*).

Definition 6.18. Let $G - \text{TCF}$ be the L_G -theory of G -fields K such that for $C := K^G$, the theory $G - \text{TCF}$ axiomatizes the following properties:

- the field K is perfect;
- the G -field K is strict;
- the G -field K is G -closed (it is a first-order property by Problem 6.2);
- the field C is PAC (it is a first-order property by Theorem 6.3).

Theorem 6.19. *Any extension of models of the theory $G - \text{TCF}$ is elementary.*

Proof. Let $K \subseteq K'$ be an extension of models of $G - \text{TCF}$ and we set:

$$C := K^G, \quad C' := (K')^G.$$

By Problem 6.3(c)(ii), it is enough to show that the extension of pure fields $C \subseteq C'$ is elementary. Since the fields C, C' are PAC, by Theorem 6.4 it is enough to show that the restriction map

$$\text{res} : \text{Gal}(C') \longrightarrow \text{Gal}(C)$$

is an isomorphism.

It is easy to see that any subfield of C' is a G -subfield of K' . It is also clear that for any two G -subfields of K' , their compositum is a G -subfield of K' as well. Hence, we obtain that C is relatively algebraically closed in C' (otherwise, the compositum field $K(C^{\text{alg}} \cap C')$ would be a proper algebraic G -field extension of K , contradicting the G -closedness of K). By Problem 10(2), the restriction map $\text{res} : \text{Gal}(K') \rightarrow \text{Gal}(K)$ is onto. We aim to show that it is one-to-one.

We consider the following commutative diagram (all the maps there are the appropriate restriction maps):

$$\begin{array}{ccc} \text{Gal}(C') & \xrightarrow{\text{res}} & \text{Gal}(C) \\ \downarrow \text{res}_{K'} & & \downarrow \text{res}_K \\ \text{Gal}(K'/C') & \xrightarrow{\text{res}_K^{K'}} & \text{Gal}(K/C). \end{array}$$

Since $K \subseteq K'$ is a G -field extension of strict G -fields, we get that the map $\text{res}_K^{K'}$ is an isomorphism. By Theorem 6.16 and Theorem 6.10, the profinite group $\text{Gal}(C)$ is projective. Therefore (since the map res is onto), there is a closed subgroup $\mathcal{G}_0 \leq \text{Gal}(C')$ such that:

$$\text{res}|_{\mathcal{G}_0} : \mathcal{G}_0 \cong \text{Gal}(C).$$

Using all the information above, we get that:

$$\text{res}_{K'}(\mathcal{G}_0) = \text{Gal}(K'/C').$$

Since the G -field K' is G -closed, the map $\text{res}_{K'}$ is a Frattini cover (see Corollary 5.7). Therefore, we obtain that $\text{Gal}(C') = \mathcal{G}_0$ and the map res is an isomorphism, which finishes the proof. \square

Corollary 6.20. *The theory $G - \text{TCF}$ is a model companion of the theory $G - \text{TF}$.*

Proof. We have already observed that any e.c. G -field is a model of $G - \text{TCF}$.

For the opposite implication, let us assume the following:

- $K \models G - \text{TCF}$;

- $\varphi(x)$ is a quantifier-free L_G -formula with parameters from K ;
- $K \subseteq K'$ is a G -field extension such that:

$$K' \models \exists x \varphi(x).$$

We aim to show that $K \models \exists x \varphi(x)$. Since the theory $G - \text{TCF}$ is inductive, there is a G -field extension $K' \subseteq K''$ such that K'' is an e.c. G -field. As noticed in the beginning of this proof, we have that $K'' \models G - \text{TCF}$. Since the formula $\varphi(x)$ is quantifier-free, we get that:

$$K'' \models \exists x \varphi(x).$$

By Theorem 6.19 (this is the crucial moment!), the G -field extension $K \subseteq K''$ is elementary. Therefore, we obtain:

$$K \models \exists x \varphi(x),$$

which finishes the proof. □

Remark 6.21. It is clear that the proof of Corollary 6.20 was quite general. One can show in the same way that for arbitrary L -theories T and T' (T inductive): if e.c. models of T are models of T' and T' is model complete, then T' is a model companion of T .

Problem List 6

Let G be a finite group and p be a prime number.

- (1) Let $K \subseteq M$ be a field extension. Show the following.
 - (a) There is a continuous homomorphism:

$$\text{res} : \text{Gal}(M) \longrightarrow \text{Gal}(K), \quad \text{res}(f) = f|_{K^{\text{alg}}}.$$
 - (b) If the field extension $K \subseteq M$ is elementary, then $\text{res} : \text{Gal}(M) \rightarrow \text{Gal}(K)$ is an epimorphism.
- (2) Find an L_G -theory T such that models of T are exactly G -closed G -fields.
- (3) Let L, L' be languages.
 - (a) Give a definition of an L' -structure, which is *definable* in an L -structure.
 - (b) Show that any G -field is definable in the pure field K^G .
 - (c) Let $K \subseteq K'$ be an extension of G -fields such that K is strict. Show the following.
 - (i) $K(K')^G = K'$.
 - (ii) The extension of G -fields $K \subseteq K'$ is elementary if and only if the extension of pure fields $K^G \subseteq (K')^G$ is elementary.
- (4) Find a subfield $K \subset \mathbb{F}_p^{\text{alg}}$ such that K is pseudofinite.
- (5) Show the following.
 - (a) The polynomial $X_1^2 + X_2^2 \in \mathbb{R}[X_1, X_2]$ is irreducible but it is not absolutely irreducible.
 - (b) The polynomial $X_1^2 + X_2^2 + 1 \in \mathbb{R}[X_1, X_2]$ is absolutely irreducible.
- (6) Let T be an L -theory (L is an arbitrary language) and we define:

$$T_f := \bigcap \{\text{Th}(M) \mid M \models T, M \text{ is finite}\}.$$
 - (a) Show that for an L -structure M , we have that $M \models T_f$ if and only if M is elementarily equivalent to an ultraproduct of finite models of T .
 - (b) Show that a field is pseudofinite if and only if it is elementarily equivalent to a non-principal ultraproduct of finite fields.
 - (c) Show that $(\mathbb{Z}, +)$ is not a pseudofinite group.
 - (d) Show that $(\mathbb{Q}, +)$ is a pseudofinite group (you may use the fact that the theory of \mathbb{Q} -vector spaces is complete).
- (7) Suppose that $R \subseteq S, R \subseteq T$ are G -field extensions (G arbitrary). Show that there is a unique G -ring structure on $S \otimes_R T$ such that the natural maps $S \rightarrow S \otimes_R T, T \rightarrow S \otimes_R T$ are G -ring homomorphisms.
- (8) Suppose that R is a G -ring (G arbitrary) which is a domain. Show that there is a unique G -field structure on the field of fractions R_0 such that $R \subseteq R_0$ is a G -ring extension.
- (9) Assume that K and M are fields such that $K \cong M$. Assume also that $n, m > 0$ are such that K has exactly m pairwise different field extensions of degree n inside a fixed algebraic closure K^{alg} . Show that M has exactly m pairwise different field extensions of degree n inside a fixed algebraic closure M^{alg} .
- (10) Let $K \subseteq M$ be a field extension such that if $a \in M \setminus K$, then a is transcendental over K . Let $F \in K[X]$. Show the following.
 - (a) F is irreducible in $K[X]$ if and only if F is irreducible in $M[X]$.
 - (b) The restriction map $\text{res} : \text{Gal}(M) \rightarrow \text{Gal}(K)$ is onto.

7. UNIVERSAL FRATTINI COVERS AND AXIOMS OF ACFA

In today's lecture, we firstly finalize the description of absolute Galois groups of fields of constants of e.c. G -fields (G finite). Then, we discuss the classical axiomatization of a model companion of the theory of difference fields (the theory ACFA).

7.1. Universal Frattini covers. We know (Corollary 5.7) that if K is a strict G -closed G -field, then the restriction map:

$$\text{res} : \text{Gal}(C) \longrightarrow G = \text{Gal}(K/C)$$

is a Frattini cover, where $C = K^G$. If K is an e.c. G -field, then we know (Theorem 6.16 and Theorem 6.10) that $\text{Gal}(C)$ is a projective profinite group. It turns out that these two properties *determine uniquely* $\text{Gal}(C)$ in terms of G . We need some more definitions (taken from [FJ]).

Let us fix a profinite group \mathcal{G} . We partially order the epimorphisms of profinite groups onto \mathcal{G} (also called *covers of \mathcal{G}*). Let $f_i : \mathcal{H}_i \rightarrow \mathcal{G}$ ($i = 1, 2$) be covers. We say that f_2 is *larger* than f_1 if there is an epimorphism $f : \mathcal{H}_2 \rightarrow \mathcal{H}_1$ such that $f_1 \circ f = f_2$. If f above is an isomorphism, then f_1 is said to be isomorphic to f_2 . An epimorphism $f_1 : \mathcal{H}_1 \rightarrow \mathcal{G}$ is called a *projective cover*, if \mathcal{H}_1 is projective. We need the following theorem and again we have to skip its proof.

Theorem 7.1 (Proposition 22.6.1 in [FJ]). *Each profinite group \mathcal{G} has a cover*

$$f : \tilde{\mathcal{G}} \longrightarrow \mathcal{G},$$

which is unique up to an isomorphism, called the universal Frattini cover, and satisfying the following equivalent conditions:

- (1) *f is a projective Frattini cover of \mathcal{G} .*
- (2) *f is the largest Frattini cover of \mathcal{G} .*
- (3) *f is the smallest projective cover of \mathcal{G} .*

In particular, each projective group is its own universal Frattini cover.

Example 7.2. Let $p \in \mathbb{P}$ and $k, n > 0$.

- There are many projective covers which are not Frattini covers, for example epimorphisms $\hat{\mathbb{Z}} \rightarrow C_n$.
- There are many Frattini covers which are not projective covers, for example epimorphisms $C_{p^2} \rightarrow C_p$ (by Problem 7.1, a finite group can not be a projective profinite group).
- An example of a universal Frattini cover is the natural projection:

$$\mathbb{Z}_p \longrightarrow C_{p^n}.$$

- We have the following universal Frattini cover:

$$\hat{F}_k(p) \longrightarrow C_{p^n}^k,$$

where $\hat{F}_k(p)$ is a *free pro- p group* on k generators, that is: it is an inverse limit of finite p -groups (called a *pro- p group*) with a specified subset $\{x_1, \dots, x_k\}$ such that any map $\{x_1, \dots, x_k\} \rightarrow \mathcal{H}$, where \mathcal{H} is a pro- p group as well, uniquely extends to a continuous homomorphism $\hat{F}_k(p) \rightarrow \mathcal{H}$. Tate showed that a pro- p

group is projective if and only if it is a free pro- p group (Proposition 22.7.6 in [FJ]).

We get the obvious conclusion of Corollary 5.7 and Theorems 6.16, 6.10, and 7.1.

Corollary 7.3. *If K is an e.c. G -field and $C = K^G$, then $\text{Gal}(C) \rightarrow G$ is the universal Frattini cover.*

Example 7.4. If K is an e.c. C_{p^i} -field, then $\text{Gal}(C) \cong \mathbb{Z}_p$. More generally, if K is an e.c. C_n -field, then $\text{Gal}(C) \cong \mathbb{Z}_n$, where

$$\mathbb{Z}_n := \mathbb{Z}_{p_1} \times \dots \times \mathbb{Z}_{p_k}$$

for $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (p_1, \dots, p_k are pairwise distinct primes and $\alpha_1 > 0, \dots, \alpha_k > 0$).

The above corollary is useful in the case when $H \leq G$ and we consider reducts of G -fields to the language of H -fields.

Example 7.5. Let p be a prime number.

(1) If $K \models C_{p^2}$ – TCF, then

$$\text{Gal}\left(K^{C_{p^2}}\right) = \widetilde{C}_{p^2} = \mathbb{Z}_p = \widetilde{C}_p.$$

By Galois theory, we obtain that:

$$p = [C_{p^2} : C_p] = [K^{C_p} : K^{C_{p^2}}] = [\text{Gal}\left(K^{C_{p^2}}\right) : \text{Gal}\left(K^{C_p}\right)].$$

Therefore, we get:

$$\text{Gal}\left(K^{C_p}\right) = p\mathbb{Z}_p \cong \mathbb{Z}_p,$$

which implies that if $(K; \sigma) \models C_{p^2}$ – TCF, then $(K; \sigma^p) \models C_p$ – TCF.

(2) If $K \models C_{p^2}^2$ – TCF, then

$$\text{Gal}\left(K^{C_{p^2}^2}\right) = \widetilde{C}_{p^2}^2 = \widehat{F}_2(p) = \widetilde{C}_p^2.$$

However, no proper closed subgroup of $\widehat{F}_2(p)$ of finite index is isomorphic to $\widehat{F}_2(p)$ (pro- p Nielsen-Schreier formula!). Therefore, if $(K; \sigma, \tau) \models C_{p^2}^2$ – TCF, then $(K; \sigma^p, \tau^p) \not\models C_p^2$ – TCF.

7.2. Axioms of ACFA. Before discussing geometric axioms for the theory G -TCF (G finite), we consider geometric axioms for the theory ACFA, which is a model companion of the theory of difference fields. So, in our terminology: ACFA = \mathbb{Z} – TCF. Let (K, σ) be a difference field, where $\sigma \in \text{Aut}(K)$ (such difference fields are called *inversive*). Then, for any tuple of variables $X = (X_1, \dots, X_n)$, σ induces an automorphism of the polynomial ring $K[X]$ and we denote this automorphism by σ as well. Assume for simplicity that K is algebraically closed. However, for a variety V , we still use the name “ K -variety” and we also often write $V(K)$ for V to make easier the subsequent generalizations to the case of an arbitrary field K .

If $V = Z(I)$ is a K -variety given by $I \trianglelefteq K[X]$, then by ${}^\sigma V$ we denote the K -variety given by the ideal $\sigma(I)$. We have the bijection map:

$$\sigma^{\times n} : K^n \longrightarrow K^n$$

and it is easy to see that (see a more general Problem 7.2):

$$\sigma^{\times n}(V(K)) = {}^\sigma V(K).$$

We denote:

$$\sigma_V := \sigma^{\times n}|_{V(K)} : V(K) \longrightarrow {}^\sigma V(K).$$

Let us consider another n -tuple of variables $Y = (Y_1, \dots, Y_n)$ and $V' = Z(I')$, where $I' \trianglelefteq K[Y]$. Then, $V \times V'$ is a K -variety as well and it is given by $(I, I') \trianglelefteq K[X, Y]$. Let W be a K -variety given by $J \trianglelefteq K[X, Y]$ such that $W \subseteq V \times V'$, which happens when $I, I' \subseteq J$ (see Problem 7.3). Then, we have the projection maps:

$$\pi : W \longrightarrow V, \quad \pi' : W \longrightarrow V'.$$

We say that π is *dominant* if $\pi(W)$ is Zariski dense in V .

We are ready now to state geometric axioms for a model companion of the theory of difference fields. By results of van den Dries and the definability of the Morley rank in the theory ACF, these axioms are first-order.

Axioms of ACFA

For any pair of K -irreducible K -varieties (V, W) , if $W \subseteq V \times {}^\sigma V$ and the projections $W \rightarrow V, W \rightarrow {}^\sigma V$ are dominant, then there is $a \in V(K)$ such that $(a, \sigma_V(a)) \in W(K)$.

Before the statement and proof of the main result, we state below Problem 7.2.

Remark 7.6. Let $K \subseteq K_1, K \subseteq K_2$ be field extensions and $\tau : K_1 \rightarrow K_2$ be a homomorphism extending σ (so, τ is not a K -algebra homomorphism!). Then, τ induces the following map:

$$\tau_V : V(K_1) \longrightarrow {}^\sigma V(K_2).$$

The main result of this part of the lecture is the following one.

Theorem 7.7 (Chatzidakis-Hrushovski). *Let (K, σ) be a difference field. Then, (K, σ) is existentially closed if and only if $(K, \sigma) \models \text{ACFA}$.*

Proof. (\Rightarrow) Let (K, σ) be an existentially closed difference field and let the pair (V, W) satisfy the assumptions of the axioms of ACFA above. It is enough to find a difference field extension $(K, \sigma) \subseteq (M, \sigma')$ and $a \in V(M)$ such that $(a, \sigma'_V(a)) \in W(M)$. Since V and W are irreducible, there are prime ideals $I \trianglelefteq K[X]$ and $J \trianglelefteq K[X, Y]$ such that $V = Z(I)$ and $W = Z(J)$. Let us define:

$$K[V] := K[X]/I, \quad K[{}^\sigma V] := K[Y]/\sigma(I), \quad K[W] := K[X, Y]/J,$$

where σ is extended to the following isomorphism of polynomial rings:

$$\sigma : K[X] \longrightarrow K[Y], \quad X \mapsto Y.$$

Since the ideals $I, \sigma(I), J$ are prime, the rings $K[V], K[{}^\sigma V], K[W]$ are domains.

Since $W \subseteq V \times {}^\sigma V$, we get $I \subseteq J, \sigma(I) \subseteq J$ and the inclusions:

$$K[X] \subset K[X, Y], \quad K[Y] \subset K[X, Y]$$

induce the K -algebra homomorphisms:

$$\alpha : K[V] \longrightarrow K[W], \quad \beta : K[{}^\sigma V] \longrightarrow K[W]$$

corresponding to the projection maps $W \rightarrow V, W \rightarrow \sigma V$. Since these projection maps are dominant, Problem 7.3 tells us that the maps α, β are one-to-one and we consider them as inclusions.

The isomorphism $\sigma : K[X] \rightarrow K[Y]$ induces the isomorphism $\tilde{\sigma} : K[V] \rightarrow K[\sigma V]$, which we consider as a monomorphism $K[V] \rightarrow K[W]$. We define:

$$K_1 := K(V), \quad K_2 := K(W), \quad \tau : K_1 \longrightarrow K_2,$$

where $K(V)$ is the fraction field of $K[V]$ (the field of rational functions on V), $K(W)$ is the fraction field of $K[W]$ (so $K_1 \subseteq K_2$ is a field extension), and τ is a homomorphism of fields which is induced by the monomorphism $\tilde{\sigma}$. Clearly, τ extends the automorphism σ of K . By Remark 7.6, τ induces a map

$$\tau_V : V(K_1) \longrightarrow \sigma V(K_2).$$

Claim For $a := (X_1 + I, \dots, X_n + I) \in V(K_1)$, we have:

$$(a, \tau_V(a)) \in W(K_2).$$

Proof of Claim. The tuple $(a, \tau_V(a))$ is considered as an element of K_2^{2n} in the following way:

$$\begin{aligned} a &= (X_1 + I, \dots, X_n + I) \mapsto (X_1 + J, \dots, X_n + J) \in K_2^n, \\ \tau_V(a) &= (Y_1 + \sigma(I), \dots, Y_n + \sigma(I)) \mapsto (Y_1 + J, \dots, Y_n + J) \in K_2^n. \end{aligned}$$

Therefore, we have:

$$(a, \tau_V(a)) = (X_1 + J, \dots, X_n + J, Y_1 + J, \dots, Y_n + J)$$

which is the usual “generic” element of $W(K_2)$. \square

This part of the proof was quite general, the crucial property of the acting group \mathbb{Z} (freeness) comes now (it is “hidden” in Problem 7.4). We have the following situation: a field tower $K \subseteq K_1 \subseteq K_2$ and a field homomorphism $\tau : K_1 \rightarrow K_2$ extending σ on K . By Problem 7.4, there is a field extension $K_2 \subseteq M$ and $\sigma' \in \text{Aut}(M)$ extending τ . Therefore, we have $a \in V(M)$ and $(a, \sigma'_V(a)) \in W(M)$, which is enough to conclude the proof of this implication (as it was noticed at the beginning of the proof).

(\Leftarrow) Suppose now that $(K, \sigma) \models \text{ACFA}$. We aim to show that (K, σ) is e.c., so let $\varphi(x)$ be a quantifier-free formula over K in the language of difference fields and assume that there is a difference field extension $(K, \sigma) \subseteq (M, \sigma')$ such that

$$(M, \sigma') \models \exists x \varphi(x).$$

We can get rid of the negations as in the proof from Example 2.4, therefore we can assume that:

$$\varphi(x) : F_1(x, \sigma(x), \dots, \sigma^m(x)) = 0 \wedge \dots \wedge F_k(x, \sigma(x), \dots, \sigma^m(x)) = 0,$$

where $F_1, \dots, F_k \in K[X, X', \dots, X^{(m)}]$ for some $m \in \mathbb{N}$ (the lengths of $X, X', \dots, X^{(m)}$ are the same as the length of the variable x). There is one more trick now to reduce the “difference degree” of these system of equations from m to 1. We introduce a new tuple of variables $z := (y, y', \dots, y^{(m-1)})$ and set

$$y := x, \quad y' := \sigma(x), \quad \dots, \quad y^{(m-1)} := \sigma^{m-1}(x).$$

Then, at the cost of expanding the length of the original tuple of variables, we reduced the difference degree to 1, so we can assume that (coming back to the original name of the logical variable):

$$\varphi(x) : F_1(x, \sigma(x)) = 0 \wedge \dots \wedge F_k(x, \sigma(x)) = 0.$$

Let t be a tuple in M such that $M \models \varphi(t)$. Then, we define (we apply σ' coordinate-wise):

$$V := \text{locus}_K(t), \quad W := \text{locus}_K(t, \sigma'(t)),$$

where, for example, $\text{locus}_K(t)$ is the smallest K -variety such that t is its rational point over M . By the properties of loci (Problem 7.5), we get that the pair of K -varieties (V, W) satisfies the assumptions of the axioms of ACFA above. Since $(K, \sigma) \models \text{ACFA}$, there is $a \in V(K)$ such that $(a, \sigma_V(a)) \in W(K)$.

By the definition of $\text{locus}_K(t, \sigma'(t))$ and since we have:

$$M \models F_1(t, \sigma'(t)) = 0 \wedge \dots \wedge F_k(t, \sigma'(t)) = 0,$$

we obtain that $W \subseteq Z(F_1, \dots, F_k)$. Since $(a, \sigma_V(a)) \in W(K)$, we obtain that

$$K \models F_1(a, \sigma(a)) = 0 \wedge \dots \wedge F_k(a, \sigma(a)) = 0.$$

Therefore, $K \models \exists x \varphi(x)$, hence (K, σ) is existentially closed which finishes the proof. \square

Problem List 7

Let K be a field and $n, m > 0$.

- (1) Show that a finite non-trivial group is not a projective profinite group.
- (2) We assume that:
 - $\sigma \in \text{Aut}(K)$;
 - V is a K -variety such that $V(K) \subseteq K^n$;
 - $K \subseteq K_1$ and $K \subseteq K_2$ are field extensions;
 - $\tau : K_1 \rightarrow K_2$ is a field homomorphism extending σ .

Show that:

$$\tau^{\times n}(V(K_1)) \subseteq {}^\sigma V(K_2).$$

- (3) We assume that:
 - the field K is algebraically closed;
 - $X = (X_1, \dots, X_n)$ and $Y = (Y_1, \dots, Y_m)$;
 - I is a prime ideal in $K[X]$ and J is a prime ideal in $K[X, Y]$;
 - $V = Z(I)$ and $W = Z(J)$;
 - the map $\pi : K^{n+m} \rightarrow K^n$ is the coordinate projection.

Show the following.

- (a) $\pi(W) \subseteq V$ if and only if $I \subseteq J$.
- (b) If $\pi(W) \subseteq V$, then $\pi(W)$ is Zariski dense in V (that is $\pi : W \rightarrow V$ is *dominant*) if and only if the corresponding ring homomorphism:

$$K[X]/I \longrightarrow K[X, Y]/J$$

is one-to-one.

- (4) Assume that $K_1 \subseteq K_2$ is a field extension and $\varphi : K_1 \rightarrow K_2$ is a field homomorphism. Show that there is a field extension $K_2 \subseteq M$ and there is $\psi \in \text{Aut}(M)$ such that ψ extends φ .
- (5) Let $K \subseteq M$ be a field extension such that the field M is algebraically closed, $a \in M^n$, and $b \in M^m$. We define:

$$I_K(a) := \{F \in K[X] \mid F(a) = 0\}, \quad \text{locus}_K(a) := Z(I_K(a)).$$

Show the following.

- (a) $I_K(a)$ is a prime ideal in $K[X]$ (so $\text{locus}_K(a)$ is a K -irreducible K -variety).
- (b) $\text{locus}_K(a)$ is the smallest K -variety V such that $a \in V(M)$.
- (c) The projection map $M^{m+n} \rightarrow M^n$ induces a dominant map:

$$\text{locus}_K(a, b) \longrightarrow \text{locus}_K(a).$$

- (d) If $\sigma \in \text{Aut}(K)$ and $\tau \in \text{Aut}(M)$ such that τ extends σ , then we have:

$$\sigma(\text{locus}_K(a)) = \text{locus}_K(\tau^{\times n}(a)).$$

8. GEOMETRIC AXIOMS AND MODEL-THEORETIC PROPERTIES OF G -TCF

In today's lecture, we describe geometric axioms for the theory G -TCF (G finite) and we also discuss some model-theoretic properties of this theory. This is the last lecture about the group actions considered in the conventional sense.

8.1. Geometric axioms of G -TCF. Let us fix a finite group G . For convenience, we denote its elements in the following way:

$$G = \{\sigma_1, \dots, \sigma_m\}, \quad \sigma_1 = e = \text{id}.$$

Let K be a G -field and $V = Z(I)$ be a K -variety, where $I \trianglelefteq K[X]$. As discussed in the previous section, for any $\sigma \in G$, we have the corresponding “ σ -twisted” K -variety ${}^\sigma V$. We define the corresponding “ G -twisted” K -variety in the following way:

$${}^G V := \sigma_1 V \times \dots \times \sigma_m V.$$

We will describe the ideal defining the K -variety ${}^G V$ aiming to show that the coordinate ring $K[{}^G V]$ has a natural G -ring structure extending the one on K . We introduce first the following tuple of variables:

$$X_G := (X_{\sigma_1}, \dots, X_{\sigma_m}), \quad X_{\sigma_1} = X.$$

Lemma 8.1. *There is a G -ring structure on $K[X_G]$ extending the one on K and such that for all $\sigma, \tau \in G$, we have:*

$$\sigma(X_\tau) = X_{\sigma\tau}.$$

Proof. It is rather clear, there is a natural action of G on X_G (considered now as a set of cardinality m) isomorphic to the regular action of G on G by left translations. Using this action, any $\sigma \in G$ induces an automorphism of $K[X_G]$ extending the action of σ on K . Since the group action axioms are satisfied on the generating set $K \cup X_G$, they are satisfied everywhere. \square

If R is a G -ring, then an ideal $J \trianglelefteq R$ is called a G -ideal, if for any $\sigma \in G$ we have $\sigma(J) = J$. We state a general fact whose proof is obvious (for any group G).

Lemma 8.2. *Suppose that R is a G -ring and $J \trianglelefteq R$ is a G -ideal. Then, there is a unique G -ring structure on R/J such that the quotient map $R \rightarrow R/J$ is a G -ring homomorphism.*

We come back now to our situation, that is $V = Z(I)$ is a K -variety and $I \trianglelefteq K[X]$. For any $\sigma \in G$, we have an isomorphism: $\sigma : K[X] \rightarrow K[X_\sigma]$ extending σ on K and we recall that:

$${}^\sigma V = Z(\sigma(I)).$$

Let us define the following ideal, which is generated by the G -orbit of I :

$$GI := (\sigma_1(I), \dots, \sigma_m(I)) \trianglelefteq K[X_G].$$

Then, we have:

$${}^G V = Z(GI),$$

and we define:

$$K[{}^G V] := K[X_G]/GI.$$

Since the ideal GI is generated by a G -invariant set (a G -orbit), GI is a G -ideal in $K[X_G]$, where the G -structure on $K[X_G]$ is given by Lemma 8.1. By Lemma 8.2, $K[X_G]$ has a natural structure of a G -ring extension of K .

To introduce the geometric axioms for the theory G -TCF, we need some more observations. Let $\sigma \in G$ and

$$\lambda_\sigma^V : {}^G V \longrightarrow \sigma({}^G V) = \sigma\sigma_1 V \times \dots \times \sigma\sigma_m V$$

be the coordinate permutation corresponding to the map:

$$\lambda_\sigma : G \longrightarrow G, \quad \lambda_\sigma(\tau) = \sigma\tau.$$

Let us assume now that W is another K -variety such that $W \subseteq {}^G V$. Then, we have:

$$\lambda_\sigma^V(W) \subseteq \sigma({}^G V), \quad \sigma W \subseteq \sigma({}^G V).$$

Some comments are in order regarding $\lambda_\sigma^V(W)$: it is a K -variety, which is rather unusual, since the *preimages* by polynomial maps of varieties are varieties again (see Problem 8.5) and it need not to hold in the case of images (for example, consider the projection of the hyperbola). However, in our case λ_σ^V is a bijective polynomial map whose inverse is a polynomial map as well (being $\lambda_{\sigma^{-1}}^V$). Hence, we have:

$$\lambda_\sigma^V(W) = (\lambda_{\sigma^{-1}}^V)^{-1}(W),$$

so it is a K -variety indeed. By Problem 8.5 and the observation above, we get the following.

Fact 8.3. *If $W = Z(J)$, then:*

$$\lambda_\sigma^V(W) = Z\left(\sigma_{X_G}^{-1}(J)\right),$$

where $\sigma_{X_G} : K[X_G] \rightarrow K[X_G]$ is a K -algebra map such that for each $\tau \in G$ we have:

$$\sigma_{X_G}(X_\tau) = X_{\sigma\tau}.$$

We are ready now to state our axioms.

Geometric axioms of G -TCF

For any pair of K -irreducible K -varieties (V, W) , IF

- $W \subseteq {}^G V = \sigma_1 V \times \dots \times \sigma_m V$;
- for all $\sigma \in G$, the projection map $W \rightarrow \sigma V$ is dominant;
- for all $\sigma \in G$, we have:

$$\lambda_\sigma^V(W) = \sigma W;$$

THEN there is $a \in V(K)$ such that $((\sigma_1)_V(a), \dots, (\sigma_m)_V(a)) \in W(K)$.

Theorem 8.4. *Let K be a G -field. Then, K is existentially closed if and only if K is a model of the geometric axioms of G -TCF.*

Proof. (\Rightarrow) Let K be an existentially closed G -field and let the pair (V, W) satisfy the assumptions of the geometric axioms of G -TCF above. It is enough to find a G -field extension $K \subseteq M$ and $a \in V(M)$ such that $((\sigma_1)_V(a), \dots, (\sigma_m)_V(a)) \in W(M)$ (we do not distinguish notationally between elements of G acting on K and on M). Since V and W are K -irreducible, there are prime ideals $I \triangleleft K[X]$ and $J \triangleleft K[X_G]$ such that $V = Z(I)$ and $W = Z(J)$.

By Fact 8.3, for each $\sigma \in G$ we have:

$$\lambda_\sigma^V(W) = Z\left(\sigma_{X_G}^{-1}(J)\right).$$

By the assumptions of the geometric axioms of G -TCF, for each $\sigma \in G$ we get:

$$\sigma_{X_G}^{-1}(J) = \sigma(J).$$

Let us consider now the G -ring extension $K \subset K[X_G]$ given by Lemma 8.1. Since σ acts on $K[X_G]$ as the composition of σ_{X_G} and σ (extended to $K[X_G]$ coefficient-wise), we obtain that J is a G -ideal. By Lemma 8.2, $K[W]$ has a G -ring structure extending the one on K . Since J is a prime ideal, $K[W]$ is a domain and the G -action on $K[W]$ uniquely extends to the fraction field $K(W)$ making it a G -field extension of K .

By the corresponding version of Claim from the proof of Theorem 7.7, we get that for a “generic point” $a \in V(K(V))$ (we regard $K(V)$ as a subfield of $K(W)$) we have:

$$((\sigma_1)_V(a), \dots, (\sigma_m)_V(a)) \in W(K(W)),$$

which finishes the proof of this implication.

(\Leftarrow) The proof follows the lines of the proof of the corresponding implication from Theorem 7.7. One just needs to notice the following: if $K \subseteq M$ is a G -field extension and $a \in M^n$, then the following pair of K -varieties:

$$\text{locus}_K(a), \quad \text{locus}_K(\sigma_1(a), \dots, \sigma_m(a))$$

satisfies the assumptions of the geometric axioms of G -TCF. \square

8.2. Model-theoretic properties of G -TCF. We finish this part of the lecture with some results concerning the model-theoretic properties of the theory G -TCF (G finite). We will skip most of the proofs.

Let $K \subseteq M$ be an extension of pure fields. We denote by $\text{alg}_M(K)$ the relative algebraic closure of K in M , which is a subfield of M containing K . Assume now that $K \subseteq M$ is a G -field extension. By Problem 8.4, $\text{alg}_M(K)$ is a G -subfield of M . If F is a prime subfield of K , then F is a G -subfield, since G acts trivially on F . Therefore, $\text{alg}_K(F)$ is a G -subfield of K . The following result classifies the completions of the theory G -TCF for a finite G , and, actually, for *any* group G such that the theory G -TCF (a model companion of the theory of G -fields) exists.

Theorem 8.5. *Let K and M be models of G -TCF, F_K be the prime subfield of K , and F_M be the prime subfield of M . Then, K and M are elementarily equivalent as G -fields if and only if $\text{alg}_K(F_K)$ and $\text{alg}_M(F_M)$ are isomorphic as G -fields.*

Remark 8.6. The description of the completions of the theory G -TCF from Theorem 8.5 may be understood as entirely analogous to the description of the completions of the theory ACF, which is not very surprising, since $\text{ACF} = \{e\}$ -TCF. For $K_1, K_2 \models \text{ACF}$, let F_i be the prime subfield of K_i ($i = 1, 2$). Then, the following are equivalent:

- (1) $K_1 \equiv K_2$;
- (2) $\text{char}(K_1) = \text{char}(K_2)$;
- (3) $F_1 \cong F_2$;
- (4) $\text{alg}_{K_1}(F_1) \cong \text{alg}_{K_2}(F_2)$.

The last condition is an exact analogue of the condition from Theorem 8.5.

Let $K \models G$ -TCF for a finite group G and $C := K^G$. We have noticed that the G -field K is definable in the pure field C (and vice versa), so it is enough to study model-theoretically the pure field C . We need one more definition.

Definition 8.7. Let M be a field and \mathcal{G} be a profinite group.

- (1) M is *bounded*, if for any $n > 0$, there are finitely many field extensions $M \subseteq M'$ of degree n in a fixed algebraic closure M^{alg} .
- (2) \mathcal{G} is *small*, if for any $n > 0$, there are finitely many closed subgroups $\mathcal{G}_0 \leq \mathcal{G}$ of index n .

By Galois theory, we immediately get the following.

Fact 8.8. A field M is bounded if and only if its absolute Galois group $\text{Gal}(M)$ is small.

Example 8.9. It is easy to see that each finite field is bounded and that \mathbb{Q} is not bounded (see also Problems 8.1–8.3).

We have the following result about the “dividing lines” in the model theory of PAC fields.

Theorem 8.10. Assume that M is a PAC field. Then, we have the following.

- (1) The theory $\text{Th}(M)$ is simple if and only if the field M is bounded.
- (2) The theory $\text{Th}(M)$ is supersimple if and only if the field M is bounded and perfect.
- (3) The theory $\text{Th}(M)$ is stable if and only if the field M is separably closed.

We will see that our field of invariants C is bounded.

Theorem 8.11. Assume that $K \models G$ -TCF (G finite) and $C = K^G$. Then, the profinite group $\text{Gal}(C)$ is finitely generated as a topological group, that is there are finitely many $g_1, \dots, g_m \in \text{Gal}(C)$ such that:

$$\text{Gal}(C) = \text{cl}(\langle g_1, \dots, g_m \rangle),$$

where cl is the topological closure.

Proof. We have the restriction map:

$$\text{res} : \text{Gal}(C) \longrightarrow G = \text{Gal}(K/C),$$

which is an epimorphism. Let $g_1, \dots, g_m \in \text{Gal}(C)$ be such that

$$\text{res}(\{g_1, \dots, g_m\}) = G.$$

We define:

$$\mathcal{H} := \text{cl}(\langle g_1, \dots, g_m \rangle).$$

By general properties of topological groups (see Problem 8.6), \mathcal{H} is a subgroup of $\text{Gal}(C)$. Clearly, we have $\text{res}(\mathcal{H}) = G$. Since the restriction map is a Frattini cover (see Corollary 5.7), we get that $\mathcal{H} = \text{Gal}(C)$, which finishes the proof. \square

Remark 8.12. The above proof actually shows that a Frattini cover of a finitely generated (topologically) profinite group is again finitely generated.

Corollary 8.13. The theory G -TCF is supersimple (G finite).

Proof. Let $K \models G\text{-TCF}$ and $C := K^G$. As argued above, it is enough to show that the theory $\text{Th}(C)$ is supersimple. By Theorem 8.10, it is enough to show that the field C is bounded. By Fact 8.8, it is enough to show that the profinite group $\text{Gal}(C)$ is small. By Theorem 8.11, $\text{Gal}(C)$ is topologically finitely generated. By Problem 8.7, $\text{Gal}(C)$ is bounded, which finishes the proof. \square

Remark 8.14. Actually, it can be shown that the SU-rank of the theory $G\text{-TCF}$ coincides with the order of G (G is still finite), and that the field of invariants C is of SU-rank 1.

Problem List 8

Let K, M be fields and G be an arbitrary group.

- (1) Assume that K is elementarily equivalent with M . Show that K is bounded if and only if M is bounded.
- (2) Assume that $K \preceq M$ and K is bounded. Show that the restriction map

$$\text{res} : \text{Gal}(M) \longrightarrow \text{Gal}(K)$$

is an isomorphism.

- (3) Show that there exists an elementary extension $\mathbb{Q} \preceq M$ such that the restriction map

$$\text{res} : \text{Gal}(M) \longrightarrow \text{Gal}(\mathbb{Q})$$

is not one-to-one.

- (4) Let $K \subseteq M$ be a G -field extension. Show that $\text{alg}_M(K)$ is a G -subfield of M .
- (5) Let $K \subseteq \Omega$ be a field extension. Let

$$V = Z(I) \subseteq \Omega^n$$

be a K -variety, where $I \trianglelefteq K[X]$. Let us also assume that

$$F = (F_1, \dots, F_n) : \Omega^m \longrightarrow \Omega^n$$

is a polynomial map, where $F_1, \dots, F_n \in K[X_1, \dots, X_m]$. Show that:

$$F^{-1}(V) = Z(F^*(I)),$$

where:

$$F^* : K[X_1, \dots, X_n] \longrightarrow K[X_1, \dots, X_m]$$

is a unique K -algebra map such that $F^*(X_i) = F_i$ for each $i \in \{1, \dots, m\}$.

- (6) Let \mathcal{G} be a topological group and $H \leq \mathcal{G}$. Show that $\text{cl}(H) \leq \mathcal{G}$, where cl is the topological closure.
- (7) Let \mathcal{G} be a profinite group, which is topologically finitely generated. Show that \mathcal{G} is small.

9. INTRODUCTION TO CATEGORY THEORY

In today's lecture, we recall basic definitions from Category Theory (categories, functors). We are not interested in the abstract theory here, but we are collecting some notions to be used later for finite group scheme actions (our main topic now).

9.1. **Categories.** Below is the formal definition of a category. We ignore here some logical issues, for example we do not specify what is a *class*: the intuition should be that it is a collection of sets which may be “too big to be a set” itself.

Definition 9.1. A *Category* \mathcal{C} consists of the following.

- A class $\text{Ob}(\mathcal{C})$, whose elements are called *objects* of \mathcal{C} .
- For each $X, Y \in \text{Ob}(\mathcal{C})$, a set $\text{Hom}(X, Y)$, whose elements are called *morphisms* between X and Y .
- For each $X, Y, Z \in \text{Ob}(\mathcal{C})$, a function

$$\circ : \text{Hom}(X, Y) \times \text{Hom}(Y, Z) \rightarrow \text{Hom}(Y, Z)$$

called the *composition* function

such that $\forall X, Y, Z, T \in \text{Ob}(\mathcal{C})$:

- (1) $(X, Y) \neq (Z, T) \Rightarrow \text{Hom}(X, Y) \cap \text{Hom}(Z, T) = \emptyset$.
- (2) $\exists! \text{id}_X \in \text{Hom}(X, X)$ such that $\forall f \in \text{Hom}(X, Y) \forall g \in \text{Hom}(Z, X)$

$$f \circ \text{id}_X = f, \text{id}_X \circ g = g.$$

- (3) $\forall f \in \text{Hom}(X, Y), \forall g \in \text{Hom}(Y, Z), \forall h \in \text{Hom}(Z, T)$

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Remark 9.2. Some warnings and conventions.

- (1) Warnings.
 - $\text{Hom}(X, Y)$ need *not* consist of functions from X to Y !
 - The “composition” map \circ need *not* be the composition of functions!
- (2) Conventions.
 - Instead of $\text{Ob}(\mathcal{C})$, we may write \mathcal{C} , so “ $X \in \mathcal{C}$ ” means “ X is an object in the category \mathcal{C} ”.
 - Instead of $f \in \text{Hom}(X, Y)$, we may write $f : X \rightarrow Y$.
 - Instead of $g \circ f$, we may write gf .
 - Instead of $\text{Hom}(X, Y)$, we may write $\text{Hom}_{\mathcal{C}}(X, Y)$.

Example 9.3. We give many examples of categories.

- (1) **Set**
 $\text{Ob}(\mathbf{Set})$ is the class of all sets, and for $X, Y \in \mathbf{Set}$, $\text{Hom}(X, Y) = Y^X$ (the set of all functions from X to Y). Formally, each function should also carry a “label” specifying its codomain, otherwise the condition (1) from Definition 9.1 is not satisfied.
- (2) **Top, Top***
 $\text{Ob}(\mathbf{Top})$ is the class of all topological spaces, morphisms are the continuous functions.
 $\text{Ob}(\mathbf{Top}_*)$ is the class of all topological spaces with a distinguished point, morphisms are the continuous functions which preserve the fixed points.

- (3) **Toph**, **Toph_{*}**
 $\text{Ob}(\mathbf{Top}) = \text{Ob}(\mathbf{Top})$, morphisms are the homotopy classes of continuous functions.
 $\text{Ob}(\mathbf{Top}_*) = \text{Ob}(\mathbf{Top}_*)$, morphisms are the homotopy classes of continuous functions which preserve the fixed points, homotopies also preserve the fixed points.
- (4) **Diff**
 $\text{Ob}(\mathbf{Diff})$ is the class of all smooth manifolds, morphisms are the smooth functions.
- (5) **AfVar_K**, where K is an algebraically closed field
 $\text{Ob}(\mathbf{AfVar}_K)$ is the class of all Zariski closed subsets of K^n (where n varies), morphisms are the restrictions of the polynomial functions.
- (6) **Mod_R**, where R is a ring (not necessarily commutative)
 $\text{Ob}(\mathbf{Mod}_R)$ is the class of all (left) R -modules, morphisms are the R -modules homomorphisms.
 We denote $\mathbf{Mod}_{\mathbb{Z}}$ by **Ab** (Abelian groups), and \mathbf{Mod}_K by **Vect_K** (vector spaces over K) if K is a field.
- (7) **Alg_R**, where R is a commutative ring
 $\text{Ob}(\mathbf{Alg}_R)$ is the class of all R -algebras (with 1), morphisms are the R -algebra homomorphisms (preserving 1).
- (8) **Grp**
 $\text{Ob}(\mathbf{Grp})$ is the class of all groups, morphisms are the group homomorphisms.
- (9) $\text{Top}(X)$, where X is a topological space
 $\text{Ob}(\text{Top}(X)) = \text{OPEN}(X)$ the set of all open subsets of X , morphisms are the inclusions.
- (10) \mathcal{C}_G , where (G, \cdot) is a group
 $\text{Ob}(\mathcal{C}_G) = \{*\}$ (a singleton), $(\text{Hom}(*, *), \circ) = (G, \cdot)$.
- (11) $\text{Def}(M)$, where M is an L -structure.
 $\text{Ob}(\text{Def}(M))$ consists of M -definable subsets of M^n ($n \in \mathbb{N}$ varies), morphisms are definable functions.

We need some more definitions.

Definition 9.4. Let \mathcal{C} and \mathcal{D} be categories.

- The category \mathcal{C} is *small*, if $\text{Ob}(\mathcal{C})$ is a set (only the categories 5., 9., 10., and 11. above are small).
- \mathcal{C}^{op} , the *opposite* category to \mathcal{C}
 $\text{Ob}(\mathcal{C}^{\text{op}}) = \text{Ob}(\mathcal{C})$, $\forall X, Y \in \mathcal{C}$, $\text{Hom}_{\mathcal{C}^{\text{op}}}(X, Y) = \text{Hom}_{\mathcal{C}}(Y, X)$.
- A morphism $f : X \rightarrow Y$ is an *isomorphism*, if there is $g : Y \rightarrow X$ such that: $gf = \text{id}_X$, $fg = \text{id}_Y$. If there is an isomorphism $X \rightarrow Y$, then we say that X and Y are *isomorphic* and write $X \cong Y$.
- A category \mathcal{C} is a *subcategory* of the category \mathcal{D} , if $\text{Ob}(\mathcal{C})$ is a subclass of $\text{Ob}(\mathcal{D})$ and for all $X, Y \in \mathcal{C}$, we have $\text{Hom}_{\mathcal{C}}(X, Y) \subseteq \text{Hom}_{\mathcal{D}}(X, Y)$.
- A subcategory \mathcal{C} is a *full* subcategory of the category \mathcal{D} , if for all $X, Y \in \mathcal{C}$, we have $\text{Hom}_{\mathcal{C}}(X, Y) = \text{Hom}_{\mathcal{D}}(X, Y)$.

Example 9.5. We give some examples of subcategories.

- **Ab** is a full subcategory of **Grp**.
- Let K be an algebraically closed field. Then, **AfVar** $_K$ is a subcategory of $\text{Def}(M)$ which is not full.
- Let **Rel** be a category, such that $\text{Ob}(\mathbf{Rel}) = \text{Ob}(\mathbf{Set})$ and morphisms are relations (note that relations can be composed). Then **Set** is a subcategory of **Rel** and is not full.
- Let U be an open subset of a topological space X . Then $\text{Top}(U)$ is a full subcategory of $\text{Top}(X)$.

9.2. **Functors.** To compare different categories, we need a notion of a functor, which is defined below.

Definition 9.6. A (*covariant*) functor F from a category \mathcal{C} into a category \mathcal{D} (notation $F : \mathcal{C} \rightarrow \mathcal{D}$) consists of:

- An assignment

$$\mathcal{C} \ni X \mapsto F(X) \in \mathcal{D}$$

- For all $X, Y \in \mathcal{C}$, a function

$$\text{Hom}_{\mathcal{C}}(X, Y) \ni f \mapsto F(f) \in \text{Hom}_{\mathcal{D}}(F(X), F(Y))$$

such that $F(fg) = F(f)F(g)$ (for appropriate f, g), and $F(\text{id}_X) = \text{id}_{F(X)}$.

A *contravariant* functor F (notation $F : \mathcal{C}^{\text{op}} \rightarrow \mathcal{D}$), is a functor from the opposite category to \mathcal{C} into \mathcal{D} , i.e. $F(fg) = F(g)F(f)$ (for appropriate f, g).

We give below some examples of functors and of important constructions related with functors.

- (1) **Cat** is the category of small categories, morphisms are functors between small categories (they can be composed).
- (2) **Forgetful functors**

$$\mathbf{Alg}_R \rightarrow \mathbf{Mod}_R \rightarrow \mathbf{Ab} \rightarrow \mathbf{Set}$$

$$\mathbf{Diff} \rightarrow \mathbf{Top} \rightarrow \mathbf{Set}$$

$$\mathbf{AfVar}_K \rightarrow \mathbf{Top} \quad (\text{Zariski topology})$$

$$\mathbf{AfVar}_{\mathbb{C}} \rightarrow \mathbf{Top} \quad (\text{Euclidean topology})$$

- (3) **Representable functors.**

For each category \mathcal{C} and $X \in \mathcal{C}$, we have two functors:

$$h_X : \mathcal{C} \rightarrow \mathbf{Set}, \quad h_X(Y) = \text{Hom}(X, Y)$$

$$h^X : \mathcal{C} \rightarrow \mathbf{Set}^{\text{op}}, \quad h^X(Y) = \text{Hom}(Y, X).$$

Both of them act on morphisms by the composition (details on Figure 1).

- (a) Let

$$F : \mathbf{Top} \rightarrow \mathbf{Toph}, \quad F_* : \mathbf{Top}_* \rightarrow \mathbf{Toph}_*$$

be the obvious functors. Then, for all $n \in \mathbb{N}$ we have the functor of the n -th homotopy group

$$\pi_n : \mathbf{Top}_* \rightarrow \mathbf{Set}, \quad \pi_n = h_{S^n} \circ F_*;$$

where S^n is the n -dimensional sphere (with an arbitrary choice of a fixed point). It is well-known that

$$\pi_1 : \mathbf{Top}_* \rightarrow \mathbf{Grp}$$

and for $n > 1$:

$$\pi_n : \mathbf{Top}_* \rightarrow \mathbf{Ab}.$$

The above formally means that there is a functor

$$\tilde{\pi}_1 : \mathbf{Top}_* \rightarrow \mathbf{Grp}$$

such that the following diagram of functors commutes:

$$\begin{array}{ccc} & & \mathbf{Grp} \\ & \nearrow \tilde{\pi}_1 & \downarrow \text{Forgetful} \\ \mathbf{Top}_* & \xrightarrow{\pi_1} & \mathbf{Set}. \end{array}$$

(b) For an algebraically closed field K , we have a functor

$$h^K : \mathbf{AfVar}_K \rightarrow (\mathbf{Alg}_K)^{\text{op}}, \quad h^K(V) = \text{Hom}_{\mathbf{AfVar}_K}(V, K).$$

We denote $h^K(V)$ by $K[V]$ (the ring of regular functions on V).

It follows from Hilbert's Nullstellensatz that we have the following isomorphism of K -algebras:

$$K[V] \cong K[X]/I(V),$$

so the definition of $K[V]$ above coincides with the definition we have been using before (as the coordinate ring of V).

10. GROUP OBJECTS AND COGROUP OBJECTS

The aim of today's lecture is to define an appropriate generalization (from the category of sets) of the notion of a group to the case of an arbitrary category.

10.1. Natural transformations and representable functors. The functors discussed last time are not exactly representable functors but rather the functors which are "already represented". To define properly the notion of a representable functor, we need to know what is an isomorphism between two functors.

Definition 10.1. Let \mathcal{C}, \mathcal{D} be categories and $F : \mathcal{C} \rightarrow \mathcal{D}, G : \mathcal{C} \rightarrow \mathcal{D}$ be functors.

- (1) ψ is a *morphism* or a *natural map* (or a *natural transformation*) between F and G (notation $\psi : F \rightarrow G$), if

$$\psi = (\psi_X : F(X) \rightarrow G(X))_{X \in \mathcal{C}}$$

such that for all $f \in \text{Hom}_{\mathcal{C}}(X, Y)$, the following diagram commutes:

$$\begin{array}{ccc} F(X) & \xrightarrow{F(f)} & F(Y) \\ \psi_X \downarrow & & \downarrow \psi_Y \\ G(X) & \xrightarrow{G(f)} & G(Y). \end{array}$$

- (2) A morphism between functors $\psi : F \rightarrow G$ is an *isomorphism*, if for all $X \in \mathcal{C}$, the morphism $\psi_X : F(X) \rightarrow G(X)$ is an isomorphism. If there is an isomorphism between the functors F and G , then, as usual, we use the notation: $F \cong G$.

Remark 10.2. It is easy to see that a morphism between functors $\psi : F \rightarrow G$ is an isomorphism if and only if there is a morphism $\varphi : G \rightarrow F$ such that $\psi \circ \varphi = \text{id}_G$ and $\varphi \circ \psi = \text{id}_F$.

Example 10.3. We have the following functors:

$$\text{id} : \mathbf{Vect}_K \longrightarrow \mathbf{Vect}_K, \quad ** : \mathbf{Vect}_K \longrightarrow \mathbf{Vect}_K;$$

where

$$* : \mathbf{Vect}_K^{\text{op}} \longrightarrow \mathbf{Vect}_K$$

is the dual space functor. Then, the classical "natural map"

$$\varphi : \text{id} \rightarrow **, \quad \varphi_V(v)(v^*) = v^*(v)$$

is really a natural map in the sense of Definition 10.1 (see Problem 9.1).

We can define now the notion of a representable functor.

Definition 10.4. Let \mathcal{C} be a category and $F : \mathcal{C} \rightarrow \mathbf{Set}$ be a functor. We say that F is *representable*, if there is $X \in \mathcal{C}$ such that $F \cong h_X$. Similarly for contravariant functors.

We will see many examples of representable functors soon.

10.2. Products and group objects. We start our discussion of group objects with a result saying that each group gives a “group functor”. The proof is presented on Figure 2.

Fact 10.5. *Let (G, \cdot) be a group. Then, there is a functor*

$$\widetilde{h}^G : \mathbf{Set}^{\text{op}} \longrightarrow \mathbf{Gps}$$

such that the following diagram of functors commutes:

$$\begin{array}{ccc} & & \mathbf{Grp} \\ & \nearrow \widetilde{h}^G & \downarrow \text{Forgetful} \\ \mathbf{Set}^{\text{op}} & \xrightarrow{h^G} & \mathbf{Set}. \end{array}$$

It can be shown that the opposite implication also holds, that is: if the functor h^X can be lifted as above to a functor to the category of groups, then the set X has a group structure and this lifting coincides with the functor \widetilde{h}^X above. Hence, groups correspond exactly to representable functors into the category of groups (more formally: to representable functors such that the liftings as above exist).

We want to do the same thing after replacing the domain category \mathbf{Set} with an arbitrary category \mathcal{C} , that is: we want to understand what kind of an additional structure an object $X \in \mathcal{C}$ should have to allow a lifting of the functor $h^X : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$ to the category of groups. After doing that, we will dualize the obtained structure to get a corresponding description for the covariant functors $h_X : \mathcal{C} \rightarrow \mathbf{Set}$.

We start with the following basic question: what is a group? It is a set G together with a function

$$\mu : G \times G \longrightarrow G,$$

which satisfies the group axioms. Therefore, the very first thing to do is to generalize the notion of a Cartesian product to an arbitrary category. The right notion is the following one.

Definition 10.6. A *product* in the category \mathcal{C} of objects $X \in \mathcal{C}$ and $Y \in \mathcal{C}$ is an object $Z \in \mathcal{C}$ together with morphisms $\pi_X : Z \rightarrow X, \pi_Y : Z \rightarrow Y$ such that:

- for each $Z' \in \mathcal{C}$ and each morphisms $f_X : Z' \rightarrow X, f_Y : Z' \rightarrow Y$,
- there is a unique morphism $f : Z' \rightarrow Z$,
- such that $f_X = f\pi_X, f_Y = f\pi_Y$.

Remark 10.7. If a product of $X, Y \in \mathcal{C}$ exists, then it is unique up to an isomorphism and it is denoted by $X \times Y$. The following diagram helps to visualize the situation:

$$\begin{array}{ccc} & Z' & \\ & \downarrow f & \\ & X \times Y & \\ & \swarrow \pi_X \quad \searrow \pi_Y & \\ X & & Y. \end{array}$$

We need the following easy general properties of products (we skip the proofs).

Lemma 10.8. *Assume that the category \mathcal{C} has products. Then, we have the following.*

- (1) *Products in the category \mathcal{C} give a functor in the sense that if $f : A \rightarrow B$ and $g : C \rightarrow D$, then we have a unique natural morphism*

$$f \times g : A \times C \longrightarrow B \times D$$

such that the following diagrams commute:

$$\begin{array}{ccc} A \times C & \xrightarrow{f \times g} & B \times D \\ \downarrow \pi_A & & \downarrow \pi_B \\ A & \xrightarrow{f} & B, \end{array} \qquad \begin{array}{ccc} A \times C & \xrightarrow{f \times g} & B \times D \\ \downarrow \pi_C & & \downarrow \pi_D \\ C & \xrightarrow{g} & D. \end{array}$$

- (2) *The product in \mathcal{C} is commutative and associative in the sense that for $X, Y, Z \in \mathcal{C}$, we have the following natural isomorphisms:*

$$X \times Y \cong Y \times X, \qquad (X \times Y) \times Z \cong X \times (Y \times Z).$$

Example 10.9. Let us see some examples of products in different categories.

- (1) **Set**, **Top**, **AfVar $_K$** .

Products are the Cartesian products. It means for the category **Top** that the Cartesian product of two topological spaces has a topology making this Cartesian product a product in the category **Top** (similarly for the category **AfVar $_K$**). Note that the Zariski topology on a product in **AfVar $_K$** is not the product topology! In other words, the forgetful functor

$$\mathbf{AfVar}_K \longrightarrow \mathbf{Top}$$

does not preserve products.

- (2) **Alg $_R$** . Products are the Cartesian products.
 (3) **Grp**. Products are the Cartesian products.
 (4) **Mod $_R$** . Products are the Cartesian products.
 (5) **Top(X)** (X is a topological space). Products are the intersections.
 (6) In the category of fields, there are usually no products (see Problem 9.2).
 (7) If G is a non-trivial group, then there are no products in the category \mathcal{C}_G (see Problem 9.3).

Remark 10.10. For any objects $Y, Z \in \mathcal{C}$, we have the following functor:

$$\text{Prod}_{Y,Z} : \mathcal{C}^{\text{op}} \longrightarrow \mathbf{Sets}, \quad \text{Prod}_{Y,Z}(X) = \text{Hom}(X, Y) \times \text{Hom}(X, Z).$$

It can be show that a product of Y and Z exists if and only if the functor $\text{Prod}_{Y,Z}$ is representable and a representing object is a product of Y and Z .

We still need some abstract properties of products, which are described below.

Definition 10.11. Suppose that the category \mathcal{C} has products and $X, Y, Z \in \mathcal{C}$.

- (1) There is a unique morphism

$$\Delta : X \longrightarrow X \times X,$$

called the *diagonal morphism*, such that the following diagram commutes:

$$\begin{array}{ccc}
 & X & \\
 \text{id}_X \swarrow & \downarrow \Delta & \searrow \text{id}_X \\
 & X \times X & \\
 \swarrow \pi_X & & \searrow \pi_X \\
 X & & X.
 \end{array}$$

- (2) For any $f : X \rightarrow Y$ and $g : X \rightarrow Z$, the morphism $(f, g) : X \rightarrow Y \times Z$ is defined as the following composition:

$$X \xrightarrow{\Delta} X \times X \xrightarrow{f \times g} Y \times Z.$$

Assume now that the category \mathcal{C} has products. Since the group associativity axiom can be expressed using a commutative diagram, we can define now the notion of a semi-group object.

Definition 10.12. A *semi-group object* in the category \mathcal{C} is a pair (G, μ) , where $G \in \mathcal{C}$, $\mu : G \times G \rightarrow G$, and the following diagram commutes:

$$\begin{array}{ccc}
 G \times G \times G & \xrightarrow{\mu \times \text{id}_G} & G \times G \\
 \text{id}_G \times \mu \downarrow & & \downarrow \mu \\
 G \times G & \xrightarrow{\mu} & G.
 \end{array}$$

It turns out that a proper definition of the notion of a neutral element is quite complicated. Firstly, the neutral element in a group is an *element* of the universe of this group, which raises the following question: what is an element of an object in a category? It can be answered in several ways, the good intuition is that an element of a variety is its rational point, but this rational point may be taken with respect to an *arbitrary* field (or even an arbitrary ring) extending the base field. However, to define properly the notion of a neutral element, we need to consider abstract “elements” of a very special kind.

As usual, to get the proper intuitions we consider the category of sets. Let $*$ \in **Set** denote an arbitrary singleton. Then, it is clear that for any $X \in \mathbf{Set}$, we have the following natural bijection:

$$X \longleftrightarrow \text{Hom}_{\mathbf{Set}}(*, X).$$

Therefore, the elements of X correspond to certain morphisms into X and the right-hand side of the above bijection will give us “elements” of an object in an arbitrary category \mathcal{C} . We still face the following question: what should play the role of the singleton $*$ in an arbitrary category \mathcal{C} ? Let us note the following categorical property of $*$, which actually describes singletons fully: for any $X \in \mathbf{Set}$, there is a unique morphism $X \rightarrow *$ (the constant map).

Definition 10.13. Let \mathcal{C} be a category.

- An object $X \in \mathcal{C}$ is an *initial object* in \mathcal{C} , if for all $Y \in \mathcal{C}$, we have

$$|\mathrm{Hom}(X, Y)| = 1.$$

- The definition of a *terminal object* is dual, i.e. $X \in \mathcal{C}$ is a terminal object in \mathcal{C} , if X is an initial object in $\mathcal{C}^{\mathrm{op}}$, that is: for all $Y \in \mathcal{C}$, we have

$$|\mathrm{Hom}(Y, X)| = 1.$$

Example 10.14. Let us see some examples of initial and terminal objects.

- (1) \emptyset is an initial object in **Set**, any singleton is a terminal object in **Set**.
- (2) \emptyset is an initial object in $\mathrm{Top}(X)$ and X is a terminal object in $\mathrm{Top}(X)$.
- (3) $\{e\}$ is both an initial and a terminal object in **Grp**, i.e. it is a *zero object* in **Grp**.
- (4) R is an initial object in \mathbf{Alg}_R . The zero ring is a terminal object in \mathbf{Alg}_R .

Remark 10.15. If an initial (resp. a terminal) object exists, then it is unique up to an isomorphism.

From now on, we assume that the category \mathcal{C} has products and terminal objects. Let us denote a fixed terminal object in \mathcal{C} by $*$. It is easy to see (Problem 9.4) that for any $X \in \mathcal{C}$, we have a natural isomorphism $X \times * \cong X$.

If $x : * \rightarrow X$ is a morphism, then for any $Y \in \mathcal{C}$ we sometimes also denote by $x : Y \rightarrow X$ the composition of the unique morphism $Y \rightarrow *$ and $x : * \rightarrow X$.

Definition 10.16. Let (G, μ) be a semi-group object in the category \mathcal{C} . A morphism $e : * \rightarrow G$ is called a *unit* (of (G, μ)) if the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{(e, \mathrm{id}_G)} & G \times G \\ (\mathrm{id}_G, e) \downarrow & \searrow \mathrm{id}_G & \downarrow \mu \\ G \times G & \xrightarrow{\mu} & G. \end{array}$$

Having the notion of a unit, it is easy now to define the categorical notion of an inverse map.

Definition 10.17. Let (G, μ) be a semi-group object in the category \mathcal{C} and $e : * \rightarrow G$ be a unit of (G, μ) . A morphism $i : G \rightarrow G$ is called an *inverse* (with respect to (G, μ, e)), if the following diagram commutes:

$$\begin{array}{ccccc} & & G & & \\ & (\mathrm{id}_G, i) \swarrow & \downarrow e & \searrow (i, \mathrm{id}_G) & \\ G \times G & \xrightarrow{\mu} & G & \xleftarrow{\mu} & G \times G. \end{array}$$

The definition of a group object is rather clear now.

Definition 10.18. A *group object* in the category \mathcal{C} is a quadruple (G, μ, e, i) such that (G, μ) is a semi-group object in \mathcal{C} , e is a unit of (G, μ) , and i is an inverse with respect to (G, μ, e) .

Example 10.19. One may wonder whether this seemingly complicated definition is a “right” one, but the following examples should convince everybody that it is the case.

- (1) In any category, a terminal object is a “trivial” group object with the obvious (unique) morphisms.
- (2) Group objects in the category **Set** are groups.
- (3) Group objects in the category **Top** are topological groups.
- (4) Group objects in the category **Toph** are called *H-groups*.
- (5) Group objects in the (naturally defined) category of smooth manifolds are Lie groups.
- (6) Group objects in the category **AfVar_K** are called *affine algebraic groups* over K .
- (7) Group objects in the category $\text{Def}(M)$ are definable groups (in M).
- (8) By Problem 9.7, group objects in the category **Grp** are commutative groups.

We state now a categorical version of Fact 10.5. The proof is analogous to the proof of Fact 10.5 and it is presented on Figure 3.

Theorem 10.20. *If (G, μ, e, i) is a group object in the category \mathcal{C} , then there is a functor*

$$\widetilde{h}^G : \mathcal{C}^{\text{op}} \longrightarrow \mathbf{Gps}$$

such that the following diagram of functors commutes:

$$\begin{array}{ccc}
 & & \mathbf{Grp} \\
 & \nearrow \widetilde{h}^G & \downarrow \text{Forgetful} \\
 \mathcal{C}^{\text{op}} & \xrightarrow{h^G} & \mathbf{Set}.
 \end{array}$$

It can be shown again that the opposite implication also holds, that is: if the functor $h^X : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$ can be lifted to a functor to the category of groups, then the object X has a group object structure and this lifting coincides with the functor \widetilde{h}^X above. Hence, group objects in \mathcal{C} correspond exactly to representable contravariant functors from \mathcal{C} into the category of groups (more formally: to representable functors such that the liftings as above exist).

10.3. Coproducts and cogroup objects. We are done with the categorical description of groups, but it is not enough for us. We also want to understand the *covariant* representable functors into the category of groups (as the fundamental group functor). Such considerations lead to the notion of a *cogroup object*. This notion is less natural, especially since there are no non-trivial “cogroups” that is the cogroup objects in the category of sets! The opposite category becomes useful now, since it is rather clear that a cogroup object in the category \mathcal{C} should be the same as a group object in the category \mathcal{C}^{op} . Hence, we need to revert all the arrows and to understand the notions of: a coproduct, an initial object (already defined), a counit, and a coinverse.

Definition 10.21. The notion of a *coproduct* is a notion which is *dual* to the notion of a product. A coproduct in the category \mathcal{C} of the objects $X, Y \in \mathcal{C}$ is denoted by $X \coprod Y$ and it comes with two morphisms:

$$\iota_X : X \longrightarrow X \coprod Y, \quad \iota_Y : Y \longrightarrow X \coprod Y;$$

which satisfy the universal condition expressed in the following commutative diagram (being dual to the diagram from Remark 10.7):

$$\begin{array}{ccc}
 & Z' & \\
 f_X \nearrow & \uparrow f & \nwarrow f_Y \\
 X & X \amalg Y & Y \\
 \iota_X \nearrow & & \nwarrow \iota_Y
 \end{array}$$

Example 10.22. Let us see some examples of coproducts.

- (1) **Set**, **Top**, **Toph**, **Diff**, **AfVar_K**.

The coproducts are the disjoint unions.

Therefore, in an arbitrary category \mathcal{C} , a coproduct of the objects $X, Y \in \mathcal{C}$ is an object representing the following functor:

$$\mathcal{C} \ni A \mapsto \text{Hom}(A, X) \cup \text{Hom}(A, Y) \in \mathbf{Set}.$$

- (2) **Set_{*}**, **Top_{*}**, **Toph_{*}**.

The coproducts are called *wedge sums*, denoted by \vee . For example, we have:

$$(S^1, *) \amalg (S^1, *) = S^1 \vee S^1 = \text{figure-eight space}.$$

- (3) **Alg_R**. The coproducts are the tensor product.
 (4) **Grp**. The coproducts are the free products.
 (5) **Mod_R**. Both the products and the coproducts coincide with the Cartesian products (in such a case, they are called the *direct sums*).
 (6) **Top(X)**. The coproducts are the unions.
 (7) In the category of fields, there are usually no coproducts (see Problem 9.2).
 (8) If G is a non-trivial group, then there are no coproducts in the category \mathcal{C}_G (see Problem 9.3).

Assume now that the category \mathcal{C} has coproducts. Then, a possible “cogroup cooperation” on $X \in \mathcal{C}$ is a morphism

$$c : X \longrightarrow X \amalg X.$$

A good intuition comes from the category **Top_{*}** (it is even better in the category **Toph_{*}**), where

$$c : (S^1, *) \longrightarrow (S^1, *) \amalg (S^1, *) = \text{figure-eight space}$$

is the “pinch map” (or the map of “shrinking the equator”).

We proceed directly now to the definition of a cogroup in a category. We assume that \mathcal{C} has coproducts and initial objects. Let us fix an initial object $\emptyset_{\mathcal{C}} \in \mathcal{C}$.

Definition 10.23. A *cogroup object* in the category \mathcal{C} is a quadruple (H, c, η, ι) (consisting of the object $H \in \mathcal{C}$, the comultiplication, the counit, and the coinverse) such that:

$$c : H \longrightarrow H \amalg H, \quad \eta : H \longrightarrow \emptyset_{\mathcal{C}}, \quad \iota : H \longrightarrow H$$

and the dual version of the diagrams from Definitions 10.12, 10.16, and 10.17 are commutative. Let us still write this diagrams explicitly. The first one expresses coassociativity.

$$\begin{array}{ccc} H \amalg H \amalg H & \xleftarrow{c \amalg \text{id}_H} & H \amalg H \\ \text{id}_H \amalg c \uparrow & & \uparrow c \\ H \amalg H & \xleftarrow{c} & H. \end{array}$$

The second one expresses being a counit, where to define e.g. the morphism (η, id_H) the *codiagonal* morphism $\nabla : H \amalg H \rightarrow H$ is used.

$$\begin{array}{ccc} H & \xleftarrow{(\eta, \text{id}_H)} & H \amalg H \\ (\text{id}_H, \eta) \uparrow & \searrow \text{id}_H & \uparrow c \\ H \amalg H & \xleftarrow{c} & H. \end{array}$$

The last diagram expresses being a coinverse, where $\eta : H \rightarrow H$ denotes the composition of the original $\eta : H \rightarrow \emptyset_{\mathcal{C}}$ with the unique morphism $\emptyset_{\mathcal{C}} \rightarrow H$ (similarly as in the case of terminal objects).

$$\begin{array}{ccccc} & & H & & \\ & \nearrow (\text{id}_H, \iota) & \uparrow \eta & \nwarrow (\iota, \text{id}_H) & \\ H \amalg H & \xleftarrow{c} & H & \xrightarrow{c} & H \amalg H. \end{array}$$

We get the following dual version of Theorem 10.20: an object $X \in \mathcal{C}$ has a cogroup object structure if and only if the functor $h_X : \mathcal{C} \rightarrow \mathbf{Set}$ lifts to the category of groups.

Example 10.24. Let us see some examples of cogroup objects.

- (1) In any category, an initial object is the “trivial” cogroup object.
- (2) In \mathbf{Set} or \mathbf{Top} , there is *only* the trivial cogroup object \emptyset , since a possible counit morphism $X \rightarrow \emptyset$ exists if and only if $X = \emptyset$.
- (3) $(S^n, *)$ is a cogroup in the category \mathbf{Toph}_* .
The comultiplication is given by the “pinch map”

$$S^n \rightarrow S^n \vee S^n.$$

In Problem 9.5, you are asked to describe the counit and the coinverse explicitly.

- (4) The cogroups in \mathbf{Grp} are exactly the free groups.

It is easy to see that any free group F_X has a cogroup structure (in the category of groups), since for any group G , we have:

$$\text{Hom}(F_X, G) \cong \text{Func}(X, G) = h^G(X)$$

and we know that $h^G(X)$ is a group. The uniqueness part is a theorem of Kan. In Problem 9.6, you are asked to describe the comultiplication, the counit, and the coinverse explicitly.

- (5) The cogroups in the category \mathbf{Alg}_K are Hopf algebras, which are our main topic here. Hopf algebras will be discussed in details during the next lecture.

Problem List 9

Let \mathcal{C} be a category, K be a field, and X be a set.

- (1) For any $V \in \mathbf{Vect}_K$, we define the following map:

$$\varphi_V : V \longrightarrow V^{**}, \quad \varphi_V(v)(v^*) = v^*(v).$$

Show that

$$\varphi := (\varphi_V)_{V \in \mathbf{Vect}_K}$$

is a natural map between the following functors:

$$\text{id} : \mathbf{Vect}_K \longrightarrow \mathbf{Vect}_K, \quad ** : \mathbf{Vect}_K \longrightarrow \mathbf{Vect}_K.$$

- (2) Let **Fields** be the category of fields.
- (a) Find $F, K \in \mathbf{Fields}$ such that a product of F and K exists in the category **Fields**.
 - (b) Find $F, K \in \mathbf{Fields}$ such that a coproduct of F and K exists in the category **Fields**.
 - (c) Find $F, K \in \mathbf{Fields}$ such that a product of F and K does not exist in the category **Fields**.
 - (d) Find $F, K \in \mathbf{Fields}$ such that a coproduct of F and K does not exist in the category **Fields**.
- (3) Let G be a non-trivial group. Show that there are no products and no coproducts in the category \mathcal{C}_G .
- (4) Let $*$ be a terminal object in the category \mathcal{C} . Show that for any $X \in \mathcal{C}$, we have a natural isomorphism

$$X \times * \cong X.$$

- (5) Let $n > 0$,

$$c : S^n \longrightarrow S^n \vee S^n$$

be the “pinch map”, and $*$ be a singleton. Find the maps:

$$\eta : S^n \longrightarrow *, \quad \iota : S^n \longrightarrow S^n$$

such that (S^n, c, η, ι) is a cogroup in the category **Toph** $_*$.

- (6) Let F_X be the free group on the set X . Find the maps:

$$c : F_X \longrightarrow F_X * F_X, \quad \eta : F_X \longrightarrow \{e\}, \quad \iota : F_X \longrightarrow F_X$$

such that (F_X, c, η, ι) is a cogroup in the category **Gps** corresponding to the group functor from Example 10.24.

- (7) Show that the group objects in **Grp** coincide with the commutative groups, where the group object morphisms come from the original group operations.

11. HOPF ALGEBRAS AND GROUP SCHEMES

In today's lecture, we will introduce the notion of a "group", which appeared in the following passage from the Introduction:

'Derivations of some kind may be still understood as "group" actions, but it has to be properly explained what does "group" mean in this context (for example, a non-trivial "group" may have no non-trivial points!), which is interesting in its own.'

This notion is connected to the cogroup objects in the category of K -algebras, such cogroup objects are classically called *Hopf algebras* (over K).

11.1. Equivalence of categories. Let us fix an algebraically closed field K . I still need to explain why cogroup objects in the category \mathbf{Alg}_K are important for us. Let us recall the representable functor:

$$h^K : (\mathbf{AfVar}_K)^{\text{op}} \longrightarrow \mathbf{Alg}_K, \quad h^K(V) = \text{Hom}_{\mathbf{AfVar}_K}(V, K),$$

where $h^K(V)$ is usually denoted by $K[V]$ (the ring of regular functions).

By Problem 10.1, this functor is *faithfully full*, that is: it induces bijections on sets of morphisms. Therefore, the image category of this functor is "the same" as the domain category. We will now describe this image (up to isomorphisms of objects) and explain what does "the same" mean in this context.

Let R be a K -algebra. By Problem 10.2, the following are equivalent:

- (1) there is $V \in \mathbf{AfVar}_K$ such that:

$$R \cong K[V]$$

(an isomorphism in the category \mathbf{Alg}_K);

- (2) R is a finitely generated K -algebra having no nilpotent elements.

Rings without nilpotent elements are called *reduced* (this term originates from algebraic geometry). Let us denote by $\mathbf{FgRedAlg}_K$ the full subcategory of \mathbf{Alg}_K whose objects are finitely generated and reduced K -algebras. By the above, there is a faithfully full functor:

$$\Theta : (\mathbf{AfVar}_K)^{\text{op}} \longrightarrow \mathbf{FgRedAlg}_K$$

such that for any $R \in \mathbf{FgRedAlg}_K$, there is $V \in \mathbf{AfVar}_K$ such that $R \cong K[V]$. The existence of such a functor means (by definition) that the categories $\mathbf{AfVar}_K^{\text{op}}$ and $\mathbf{FgRedAlg}_K$ are *equivalent*. We can always move the opposite category to the other side of functors/equivalences etc., so the categories \mathbf{AfVar}_K and $\mathbf{FgRedAlg}_K^{\text{op}}$ are equivalent as well.

In particular, group objects in \mathbf{AfVar}_K (algebraic groups) correspond to certain cogroup objects in \mathbf{Alg}_K (such that the underlying K -algebra is finitely generated and reduced). We will be interested in arbitrary cogroup objects in \mathbf{Alg}_K for an arbitrary field (or even: an arbitrary commutative ring) K .

11.2. Hopf algebras and affine group schemes. Let us take an algebraic group (G, μ, e, i) , which is a group object in the category \mathbf{AfVar}_K . Note that (G, μ) is an actual group, since products in \mathbf{AfVar}_K are Cartesian products, but (G, μ) is *not* a topological group by Example 10.9(1). For a morphism $f : V \rightarrow W$ in the category

\mathbf{AfVar}_K , we denote by $f^* : K[W] \rightarrow K[V]$ the image of this morphisms by the coordinate ring functor. Then, the quadruple $(K[G], \mu^*, e^*, i^*)$ is a cogroup object in the category \mathbf{Alg}_K and let us look at the maps μ^*, e^*, i^* more closely:

$$\mu^* : K[G] \longrightarrow K[G \times G] = K[G] \otimes_K K[G], \quad e^* : K[G] \rightarrow K, \quad i^* : K[G] \rightarrow K[G].$$

These maps fit to the commutative diagrams described for an arbitrary category in Definition 10.23. These considerations lead to the following definition.

Definition 11.1. Let R be a (unital commutative) ring. A *Hopf algebra* over R is a cogroup object in the category \mathbf{Alg}_R , that is: it is a quadruple (H, c, η, ι) such that:

$$c : H \longrightarrow H \otimes_R H, \quad \eta : H \longrightarrow R, \quad \iota : H \longrightarrow H$$

are R -algebra homomorphisms and the following diagrams are commutative, where “ \otimes ” stands for “ \otimes_R ”:

$$\begin{array}{ccc} H \otimes H \otimes H & \xleftarrow{c \otimes \text{id}_H} & H \otimes H \\ \text{id}_H \otimes c \uparrow & & \uparrow c \\ H \otimes H & \xleftarrow{c} & H, \\ \\ H & \xleftarrow{(\eta, \text{id}_H)} & H \otimes H \\ (\text{id}_H, \eta) \uparrow & \searrow \text{id}_H & \uparrow c \\ H \otimes H & \xleftarrow{c} & H, \\ \\ H \otimes H & \xrightarrow{(\text{id}_H, \iota)} & H & \xleftarrow{(\iota, \text{id}_H)} & H \otimes H \\ & \uparrow \eta & & & \\ & H & & & \end{array}$$

Let us consider again an algebraically closed field K and an affine algebraic group G . Then, $K[G]$ is a Hopf algebra and we have the following natural bijective correspondence (Problem 10.3):

$$G(R) \longleftrightarrow \text{Hom}_{\mathbf{Alg}_K}(K[G], R),$$

where $G(R)$ stands for the set of R -rational points of G , that is: the zeroes in R^n of the ideal $I(G) \trianglelefteq K[X]$, where $X = (X_1, \dots, X_n)$. Since $K[G]$ is a Hopf algebra (a cogroup object in \mathbf{Alg}_K), $G(R)$ is a group. Therefore, the affine algebraic group G can be considered as the (group) *functor of rational points*:

$$G : \mathbf{Alg}_K \longrightarrow \mathbf{Gps}.$$

This motivates the following generalization.

Definition 11.2. Let R be a ring. An *affine group scheme* over R is a representable functor

$$\mathbf{Alg}_R \longrightarrow \mathbf{Gps}.$$

Remark 11.3. A representable functor can be identified with an object representing it (this is *Yoneda Lemma*, which we skip), so an affine group scheme over R is basically the same as a (representing) Hopf algebra over R .

Example 11.4. We will see several examples of group schemes. Let K be an algebraically closed field and $n > 0$.

- (1) The set K^n considered as an affine algebraic variety is usually denoted by \mathbb{A}^n (or \mathbb{A}_K^n) and called the *affine n -space*. It is clear that:

$$K[\mathbb{A}^n] = K[X_1, \dots, X_n].$$

Since \mathbb{A}^1 (called also the *affine line*) has the structure of an affine algebraic group (with the field addition), $K[X]$ has the natural corresponding Hopf algebra structure, which is calculated on Figure 4.

For a ring R , let us consider the following functor:

$$\mathbb{G}_{a,R} : \mathbf{Alg}_R \longrightarrow \mathbf{Gps}, \quad \mathbb{G}_{a,R}(T) = (T, +).$$

It is clear that it is a group scheme and the corresponding Hopf algebra is the same one as in the case of $R = K$ above (just all the instances of “ K ” should be replaced with “ R ”). It is called the *additive group scheme* (over R). We also denote:

$$\mathbb{G}_a := \mathbb{G}_{a,\mathbb{Z}}.$$

- (2) We consider now the multiplicative group. As such:

$$K^* = \{a \in K \mid a \neq 0\}$$

is a *Zariski open* subset of K . However, by the standard trick (appearing also in Example 2.4), we can identify K^* with the following Zariski closed subset of \mathbb{A}^2 (called also the *affine plane*):

$$C := \{(a, t) \in K^2 \mid at = 1\},$$

which is the hyperbola. It is also clear that:

$$K[C] = K[X, 1/X].$$

Since C has the structure of an affine algebraic group (with the field multiplication), $K[X, 1/X]$ has the natural corresponding Hopf algebra structure, which is calculated on Figure 5.

For a ring R , let us consider the following functor:

$$\mathbb{G}_{m,R} : \mathbf{Alg}_R \longrightarrow \mathbf{Gps}, \quad \mathbb{G}_{m,R}(T) = (T^*, \cdot).$$

It is clear that it is a group scheme and the corresponding Hopf algebra is the same one as in the case of $R = K$ above (similarly as in Item (1)). It is called the *multiplicative group scheme* (over R). We also denote:

$$\mathbb{G}_m := \mathbb{G}_{m,\mathbb{Z}}.$$

- (3) We consider the functor:

$$\ker(\text{Fr}) : \mathbf{Alg}_{\mathbb{F}_p} \longrightarrow \mathbf{Gps}, \quad \ker(\text{Fr})(R) = \{r \in R \mid r^p = 0\}.$$

In Problem 10.6, you are asked to show that $\ker(\text{Fr})$ is a group scheme over \mathbb{F}_p .

Problem List 10

Let K be an algebraically closed field, p be a prime number, and $n \in \mathbb{N}_{>0}$.

- (1) Show that the representable functor:

$$h^K : (\mathbf{AfVar}_K)^{\text{op}} \longrightarrow \mathbf{Alg}_K, \quad h^K(V) = \text{Hom}_{\mathbf{AfVar}_K}(V, K),$$

is *faithfully full*, that is: it induces bijections on the sets of morphisms.

- (2) Let $R \in \mathbf{Alg}_K$. Show that the following are equivalent:

- (a) there is $V \in \mathbf{AfVar}_K$ such that:

$$R \cong K[V]$$

(an isomorphism in \mathbf{Alg}_K);

- (b) R is a finitely generated K -algebra having no nilpotent elements.

- (3) Let $V \in \mathbf{AfVar}_K$. Show that we have the following natural bijective correspondence:

$$V(R) \longleftrightarrow \text{Hom}_{\mathbf{Alg}_K}(K[V], R),$$

where $V(R)$ stands for the set of R -rational points of V , that is: the zeroes in R^n of the ideal $I(V) \triangleleft K[X]$, where $X = (X_1, \dots, X_n)$.

- (4) Show that:

$$K[\text{GL}_n(K)] \cong K[X_{1,1}, \dots, X_{n,n}, T] / (T \det((X_{i,j})_{i,j}) - 1)$$

and determine the Hopf algebra structure on $K[\text{GL}_n(K)]$, which corresponds to the algebraic group $\text{GL}_n(K)$.

- (5) Show that:

$$\text{GL}_n : \mathbf{Alg}_{\mathbb{Z}} = \mathbf{Rings} \longrightarrow \mathbf{Gps}, \quad \text{GL}_n(R) = \{A \in M_n(R) \mid \det(A) \in R^*\}$$

is a group scheme over \mathbb{Z} .

- (6) Show that:

$$\ker(\text{Fr}) : \mathbf{Alg}_{\mathbb{F}_p} \longrightarrow \mathbf{Gps}, \quad \ker(\text{Fr})(R) = \{r \in R \mid r^p = 0\}.$$

is a group scheme over \mathbb{F}_p .

12. ACTIONS OF FINITE GROUP SCHEMES

In today's lecture, we finally define the notion of actions of (finite) group schemes, whose model theory we aim to study, similarly as we studied the model theory of actions of finite groups on fields.

12.1. More examples and structure constants. Firstly, we give some examples of classical functors which are or are *not* group schemes (although they may look as such at first sight). It is not very much related to the main topic, but it is still interesting and should provide a better understanding of group schemes.

Example 12.1. We consider the following classical functors. Let $n > 0$ and we recall that the category of rings coincides with the category of \mathbb{Z} -algebras and we will use the notion for the latter.

- (1) *General linear group and special linear group.*

Let us consider the following functors:

$$\mathrm{GL}_n : \mathbf{Alg}_{\mathbb{Z}} \longrightarrow \mathbf{Gps}, \quad R \mapsto \mathrm{Aut}_{\mathrm{Mod}_R}(R^n),$$

$$\mathrm{SL}_n : \mathbf{Alg}_{\mathbb{Z}} \longrightarrow \mathbf{Gps}, \quad R \mapsto \{f \in \mathrm{GL}_n(R) \mid \det(f) = 1\}.$$

If K is an algebraically closed field, then we consider the general linear group $\mathrm{GL}_n(K)$ as an affine variety. We have that

$$\mathrm{GL}_n(K) = \{A \in M_n(K) \mid \det(A) \neq 0\}$$

is a *Zariski open* subset of $M_n(K) = \mathbb{A}^{n^2}$ (the determinant function is a polynomial function). Similarly as in Example 11.4(2), it can be identified with the following Zariski closed subset of \mathbb{A}^{n^2+1} :

$$\{(A, t) \in M_n(K) \times K \mid \det(A)t = 1\}.$$

The interpretation of $\mathrm{GL}_n(K)$ as a Zariski closed subset of \mathbb{A}^{n^2+1} also gives the *correct* interpretation of $\mathrm{GL}_n(R)$ for an arbitrary ring R as:

$$\mathrm{GL}_n(R) = \{A \in M_n(R) \mid \det(A) \in R^*\}!$$

In Problem 10.5, you are asked to show that GL_n is a group scheme over \mathbb{Z} . We clearly have:

$$\mathrm{GL}_1 \cong \mathbb{G}_m.$$

Similarly, SL_n is a group scheme over \mathbb{Z} as well.

For the next two items, we need to notice that:

$$Z(\mathrm{GL}_n(R)) = R^*I \cong R^*,$$

$$Z(\mathrm{SL}_n(R)) = R^*I \cap \mathrm{SL}_n(R) \cong \mu_n(R) := \{r \in R^* \mid r^n = 1\}.$$

- (2) *Projective general linear group.*

Let us consider the following functor

$$\mathbf{Alg}_{\mathbb{Z}} \longrightarrow \mathbf{Gps}, \quad R \mapsto \mathrm{GL}_n(R)/Z(\mathrm{GL}_n(R)).$$

This functor, which we may be tempted to call PGL_n , is *not* a group scheme (that is: it is not representable) for the following reasons. There is the following *adjoint representation* map:

$$\mathrm{Ad} : \mathrm{GL}_n \longrightarrow \mathrm{GL}_{n^2}, \quad \mathrm{Ad}_R(A)(B) = ABA^{-1},$$

where R is a ring, $A \in \mathrm{GL}_n(R)$, and $B \in M_n(R) = R^{n^2}$. For any ring R , we have:

$$\ker(\mathrm{Ad}_R) = Z(\mathrm{GL}_n(R)).$$

It can be shown that if K is an algebraically closed field, then the image:

$$\mathrm{Ad}_K(\mathrm{GL}_n(K)) < \mathrm{GL}_{n^2}(K)$$

is Zariski closed, so this image has a structure of an algebraic group. Similarly as in Problem 10.5, there is a group scheme over \mathbb{Z} , which is denoted by PGL_n , such that for all rings R we have a natural isomorphism:

$$\mathrm{PGL}_n(K) \cong \mathrm{Ad}_K(\mathrm{GL}_n(K)).$$

In the case of $n = 2$, this group scheme is represented by:

$$H_0 := \mathbb{Z} \left[\frac{XY}{d}, \frac{XZ}{d}, \frac{XT}{d}, \frac{YZ}{d}, \frac{YT}{d}, \frac{YZ}{d}, \frac{X^2}{d}, \frac{Y^2}{d}, \frac{Z^2}{d}, \frac{T^2}{d} \right],$$

where $d := XT - YZ$ and the Hopf algebra structure on H_0 is induced from the Hopf algebra H giving GL_2 :

$$H := \mathbb{Z} \left[X, Y, Z, T, \frac{1}{XT - YZ} \right]$$

representing the group scheme GL_2 (so H_0 is a *Hopf subalgebra* of H , which is OK, since: group scheme quotients correspond to Hopf subalgebras, and subgroup schemes correspond to Hopf algebra quotients).

For any ring R , Ad_R induces the following monomorphism:

$$\mathrm{GL}_n(R)/Z(\mathrm{GL}_n(R)) \longrightarrow \mathrm{PGL}_n(R),$$

which is an isomorphism if $R = K$ is a field. However, Ad_R need not be onto and in general we have the following exact sequence (the word “exact” here means that the image of each arrow coincides with the kernel of the next arrow):

$$1 \longrightarrow \mathrm{GL}_n(R)/Z(\mathrm{GL}_n(R)) \longrightarrow \mathrm{PGL}_n(R) \longrightarrow \mathrm{Pic}(R) \longrightarrow 1.$$

Therefore, the “difference” between $\mathrm{GL}_n(R)/Z(\mathrm{GL}_n(R))$ and $\mathrm{PGL}_n(R)$ is measured by the *Picard group* of R , which, for example, for a Dedekind ring R coincides with the ideal class group $\mathrm{Cl}(R)$. Hence if R is a field or a local ring or a PID ring, then we have:

$$\mathrm{PGL}_n(R) \cong \mathrm{GL}_n(R)/Z(\mathrm{GL}_n(R)).$$

(3) *Projective special linear group.*

Let us consider the following functor

$$\mathrm{PSL}_n : \mathbf{Alg}_{\mathbb{Z}} \longrightarrow \mathbf{Gps}, \quad R \mapsto \mathrm{SL}_n(R)/Z(\mathrm{SL}_n(R)).$$

This is *not* a group scheme and the quotient of the group scheme SL_n by the normal group subscheme $Z(\mathrm{SL}_n)$ (all these notions make a formal sense, but I will not give the definitions here) coincides with the group scheme PGL_n as in Item (1). The difference can be already observed on the level of fields and it

is given by the following commutative diagram (see Problem 11.6), where each row is exact and each column is exact:

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \mu_n(K) & \xrightarrow{\cong} & K^* & \xrightarrow{x \mapsto x^n} & (K^*)^n & \longrightarrow & 1 \\
 & & \downarrow x \mapsto xI & & \downarrow x \mapsto xI & & \downarrow \cong & & \\
 1 & \longrightarrow & \mathrm{SL}_n(K) & \xrightarrow{\cong} & \mathrm{GL}_n(K) & \xrightarrow{\det} & K^* & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 1 & \longrightarrow & \mathrm{PSL}_n(K) & \longrightarrow & \mathrm{PGL}_n(K) & \longrightarrow & K^*/(K^*)^n & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
 \end{array}$$

We define now a type of group schemes, which generalizes the notion of a finite group and this is the type which is most interesting for us.

Definition 12.2. Let k be a field. A *finite group scheme* over k is an affine group scheme over k such that the corresponding Hopf algebra is finite-dimensional as a vector space over k .

I will give now some examples of finite groups schemes.

Example 12.3. Let k be a base field and $n > 0$.

(1) *Constant finite group schemes.*

Let (G, μ) be a finite group and we set $H := k^G$. The Hopf algebra structure on H should come from μ :

$$\mu^* : k^G \longrightarrow k^{G \times G}, \quad \mu^*(f) = f \circ \mu.$$

By Problem 11.2, if X and Y are finite sets, then we get the following isomorphism of k -algebras, which is “natural in X and Y ”:

$$k^{X \times Y} \cong k^X \otimes_k k^Y$$

(this is a *Stone-Weierstrass* type statement: the right-hand side above corresponds to functions of the form

$$(x, y) \mapsto f_1(x)g_1(y) + \dots + f_n(x)g_n(y)$$

for some $n > 0$, $f_i : X \rightarrow k$, and $g_i : Y \rightarrow k$). Using Problem 11.2, we get that μ^* is a *cooperation* on $H := k^G$:

$$\mu^* : H \longrightarrow H \otimes_k H$$

(all tensor products are taken over k). Since μ is associative, we have:

$$\mu \circ (\mu \times \mathrm{id}_G) = \mu \circ (\mathrm{id}_G \times \mu).$$

Applying the representable contravariant functor h^k , we get that the following diagram commutes:

$$\begin{array}{ccc} H \otimes_k H \otimes_k H & \xleftarrow{\mu^* \otimes \text{id}_H} & H \otimes_k H \\ \text{id}_H \otimes \mu^* \uparrow & & \uparrow \mu^* \\ H \otimes_k H & \xleftarrow{\mu^*} & H. \end{array}$$

that is μ^* is *coassociative*.

The neutral element in G can be understood as a map

$$e : \{\text{id}\} \longrightarrow G.$$

We get the corresponding *counit* map:

$$e^* : H = k^G \longrightarrow k = k^{\{\text{id}\}}$$

fitting to the following commutative diagram:

$$\begin{array}{ccc} H & \xleftarrow{e^* \cdot \text{id}_H} & H \otimes_k H \\ \text{id}_H \cdot e^* \uparrow & \swarrow \text{id}_H & \uparrow \mu^* \\ H \otimes_k H & \xleftarrow{\mu^*} & H. \end{array}$$

Finally, let us consider the inverse map on G :

$$i : G \longrightarrow G.$$

It induces the following *coinverse* map:

$$i^* : H = k^G \longrightarrow H = k^G$$

fitting to the following commutative diagram:

$$\begin{array}{ccccc} & & H & & \\ & \text{id}_H \cdot i^* \nearrow & \uparrow e^* & \nwarrow i^* \cdot \text{id}_H & \\ H \otimes_k H & \xleftarrow{\mu^*} & H & \xrightarrow{\mu^*} & H \otimes_k H. \end{array}$$

Let

$$\mathbf{G} : \mathbf{Alg}_k \longrightarrow \mathbf{Gps}$$

be the group scheme represented by the Hopf algebra k^G . By Problem 11.1, for any *connected* (that is: without non-trivial idempotents) $R \in \mathbf{Alg}_k$, we have a natural isomorphism $\mathbf{G}(R) \cong G$.

Let $\{\chi_g \mid g \in G\}$ be a k -basis of k^G consisting of characteristic functions ($\chi_g(h) = \delta_h^g$: Kronecker's delta). Then, we have (computed on Figure 6):

$$\mu^*(\chi_g) = \sum_{hk=g} \chi_h \otimes \chi_k.$$

For any $g \in G$ we have:

$$e^*(\chi_g) = \chi_g(e) = \delta_h^g,$$

and it is easy to see that

$$i^*(\chi_g) = \chi_{g^{-1}}.$$

(2) *Kernels of powers of Frobenius.*

Extending Example 11.4(3) and changing the notation a bit we define:

$$\alpha_{p^n} : \mathbf{Alg}_{\mathbb{F}_p} \longrightarrow \mathbf{Gps}, \quad \alpha_{p^n}(R) = \{r \in R \mid r^{p^n} = 0\}.$$

Similarly as in Example 11.4(3), α_{p^n} is a group scheme represented by

$$\mathbb{F}_p[\varepsilon] := \mathbb{F}_p[X]/(X^{p^n})$$

(not to overload the notation, we still use “ ε ” instead of e.g. “ ε_n ”) and

$$c : \mathbb{F}_p[\varepsilon] \longrightarrow \mathbb{F}_p[\varepsilon] \otimes_{\mathbb{F}_p} \mathbb{F}_p[\varepsilon], \quad c(\varepsilon) = \varepsilon \otimes 1 + 1 \otimes \varepsilon$$

(this map is well-defined again, since $\text{char}(\mathbb{F}_p) = p$).

Let $\{1, \varepsilon, \dots, \varepsilon^{p^n-1}\}$ be a basis of $\mathbb{F}_p[\varepsilon]$ considered as an \mathbb{F}_p -linear space. Then we have the following:

$$\begin{aligned} c(\varepsilon^i) &= c(\varepsilon)^i \\ &= (\varepsilon \otimes 1 + 1 \otimes \varepsilon)^i \\ &= \sum_{k=0}^i \binom{i}{k} \varepsilon^k \otimes \varepsilon^{i-k}. \end{aligned}$$

It is easy to see that we also have:

$$\eta(\varepsilon^i) = \delta_0^i, \quad \iota(\varepsilon^i) = (-1)^i \varepsilon^i.$$

There is a standard name to some parameters from the base field, which appeared above.

Definition 12.4. Let H be a finite-dimensional Hopf algebra over a field k and $\{b_1, \dots, b_m\}$ be a basis of H over k (as a k -linear space). Then, the *structure constants* $(\nu_i^{j,k})_{i,j,k}$ of the comultiplication c (with respect to this chosen basis) are the elements of k , which are given by the following formula ($i \leq m$):

$$c(b_i) = \sum_{j,k} \nu_i^{j,k} b_j \otimes b_k.$$

Similarly, we can define the structure constants for the coinverse map and the counit map.

Remark 12.5. One can describe the coassociativity axiom using the structure constants in the following way:

$$\nu_k^{i,j} \nu_i^{m,n} = \nu_k^{m,i} \nu_i^{n,j}.$$

Example 12.6. Structure constants for finite group schemes from Example 12.3.

(1) For $H = k^G$ and $k, h, g \in G$, we have the following ($hk = \mu(h, k) \in G$):

$$\nu_g^{h,k} = \delta_g^{hk}.$$

(2) For α_{p^n} and $i, j, k < p^n$, we have the following:

$$\nu_i^{j,k} = \binom{i}{k} \delta_i^{j+k}.$$

12.2. Hopf algebra coactions. Let us fix two covariant functors (instead of the category \mathbf{Alg}_k we could have taken an arbitrary domain category):

$$\mathbf{G} : \mathbf{Alg}_k \longrightarrow \mathbf{Gps}, \quad \mathbf{X} : \mathbf{Alg}_k \longrightarrow \mathbf{Set}.$$

An *action* of \mathbf{G} on \mathbf{X} is a natural transformation

$$a : \mathbf{G} \times \mathbf{X} \longrightarrow \mathbf{X}$$

such that for each $T \in \mathbf{Alg}_k$, the map:

$$a_T : \mathbf{G}(T) \times \mathbf{X}(T) \longrightarrow \mathbf{X}(T)$$

is a group action.

Assume now that the functor \mathbf{G} is represented by a Hopf algebra H over k (so \mathbf{G} is an affine group scheme over k) and \mathbf{X} is represented by the k -algebra R (so \mathbf{X} is an *affine scheme* over k). In such a case, we will use the following notation (the reasons for this notation will not be explained in this course):

$$\mathbf{G} = \text{Spec}(H), \quad \mathbf{X} = \text{Spec}(R).$$

Since the usual group action axioms (the identity axiom and the mixed associativity axiom) are expressed by the following commutative diagrams (a group (G, μ) acts on a set X by $a : G \times X \rightarrow X$):

$$\begin{array}{ccc} X \times G & \xleftarrow{(id, e)} & X \\ a \downarrow & \swarrow id_X & \\ X & & \end{array} \quad \begin{array}{ccc} X \times G & \xleftarrow{id_X \times \mu} & X \times G \times G \\ a \downarrow & & \downarrow a \times id_G \\ X & \xleftarrow{a} & X \times G \end{array}$$

we get that an action of \mathbf{G} on \mathbf{X} corresponds to a *coaction* of the Hopf algebra H on R , that is to a k -algebra map:

$$\partial : R \longrightarrow R \otimes_k H$$

such that the following diagrams (expressing the counit condition and the mixed coassociativity conditions) commute:

$$\begin{array}{ccc} R \otimes_k H & \xrightarrow{id_R \cdot \eta} & R = R \otimes_k k \\ \partial \uparrow & \searrow id_R & \\ R & & \end{array} \quad \begin{array}{ccc} R \otimes_k H & \xrightarrow{id_R \otimes c} & R \otimes_k H \otimes_k H \\ \partial \uparrow & & \uparrow \partial \otimes id_H \\ R & \xrightarrow{\partial} & R \otimes_k H. \end{array}$$

We are interested in the model theory of *actions of finite group schemes on fields*, which is the situation as above after assuming that:

- $R = K$ is a field;
- $\dim_k H$ is finite.

Before the next example, we need one definition.

Definition 12.7. Let k be a field and $R \in \mathbf{Alg}_k$.

- (1) A map $\partial : R \rightarrow R$ is called a *derivation* (on R), if for all $x, y \in R$, we have the following:
 - $\partial(x + y) = \partial(x) + \partial(y)$ (∂ is *additive*);

- $\partial(xy) = x\partial(y) + y\partial(x)$ (∂ satisfies the *Leibniz rule*).
- (2) A derivation $\partial : R \rightarrow R$ is called a *k-derivation*, if it is *k-linear* (equivalently: $\partial(k) = 0$).

Example 12.8. We give two examples of finite group scheme actions on (the functors represented by) rings. In both cases, we first interpret the *k*-algebra map ∂ (using a fixed basis) and then understand the additional Hopf algebra coaction conditions.

- (1) Let us fix a finite group (G, μ) and set $H := k^G$. We also fix a *k*-algebra R . Then, the action of $\text{Spec}(H)$ on $\text{Spec}(R)$ corresponds to a *k*-algebra map

$$\partial : R \rightarrow R \otimes_k H$$

satisfying two additional conditions as above. We analyze first such maps in general and then interpret these two additional conditions.

Let us take the basis of H consisting of characteristic functions $\{\chi_g \mid g \in G\}$ (see Example 12.3(1)). Then an *arbitrary* map $\partial : R \rightarrow R \otimes_k H$ corresponds to a sequence of maps $(\partial_g : R \rightarrow R)_{g \in G}$ such that for all $r \in R$, we have:

$$\partial(r) = \sum_{g \in G} \partial_g(r) \otimes \chi_g.$$

We have:

$$R \otimes_k H = \sum_{g \in G} R(1 \otimes \chi_g) \cong_R R^m,$$

where the last isomorphism is an isomorphism of *R*-algebras, since the characteristic functions satisfy the following “orthogonality conditions” ($h, g \in G$):

$$\chi_g^2 = \chi_g, \quad \chi_g \chi_h = \delta_h^g \quad (\text{Kronecker's delta}).$$

Therefore, it is easy to see that $\partial : R \rightarrow R \otimes_k H$ is a *k*-algebra map if and only if each $\partial_g : R \rightarrow R$ is a *k*-algebra map.

We interpret now the counit condition. Recall from Example 12.3(1) that for all $g \in G$, we have:

$$\eta(\chi_g) = \delta_e^g.$$

Let us take $r \in R$ and “travel up and right” in the diagram responsible for the counit axiom:

$$\begin{aligned} (\text{id}_R \cdot \eta)(\partial(r)) &= (\text{id}_R \cdot \eta) \left(\sum_{g \in G} \partial_g(r) \otimes \chi_g \right) \\ &= \sum_{g \in G} \partial_g(r) \eta(\chi_g) \\ &= \sum_{g \in G} \partial_g(r) \delta_e^g \\ &= \partial_e(r). \end{aligned}$$

Therefore, $\partial : R \rightarrow R \otimes_k H$ satisfies the counit condition if and only if $\partial_e = \text{id}_R$.

We calculate on Figure 7 that the mixed coassociativity condition for $\partial : R \rightarrow R \otimes_k H$ means exactly that for all $g, h \in G$ we have:

$$\partial_g \circ \partial_h = \partial_{gh}.$$

Therefore, group scheme actions of $\text{Spec}(k^G)$ on $\text{Spec}(R)$ correspond exactly to action of G on R by k -algebra automorphisms.

- (2) Let us consider the group scheme α_{p^n} (see Example 12.3(2)), which is represented by the Hopf algebra

$$\mathbb{F}_p[\varepsilon] := \mathbb{F}_p[X]/(X^{p^n}).$$

Let

$$\partial : R \rightarrow R \otimes_{\mathbb{F}_p} \mathbb{F}_p[\varepsilon], \quad \partial(r) = \sum_{i=0}^{p^n-1} \partial_i(r) \otimes \varepsilon^i,$$

where each ∂_i is a map from R to R similarly as in Item (1) above.

We calculate on Figure 8 that ∂ is a \mathbb{F}_p -algebra map if and only if the following holds:

- for each i , ∂_i is an additive map;
- for each i and $x, y \in R$, we have:

$$\partial_i(xy) = \sum_{j+k=i} \partial_j(x) \partial_k(y).$$

In particular, ∂_0 is a \mathbb{F}_p -algebra map and ∂_1 is a “derivation of ∂_0 ”, that is:

$$\partial_1(xy) = \partial_0(x) \partial_1(y) + \partial_0(y) \partial_1(x).$$

Similarly as in Item (1), a \mathbb{F}_p -algebra map $\partial : R \rightarrow R \otimes_{\mathbb{F}_p} \mathbb{F}_p[\varepsilon]$ satisfies the counit condition if and only if $\partial_0 = \text{id}_R$. In such a case, ∂_1 is a derivation on R , and the whole sequence $(\partial_i)_{i < p^n}$ is sometimes called a *truncated Hasse-Schmidt derivation* on R .

Finally, let us consider the mixed coassociativity condition. For $r \in R$, firstly we “travel up and right” in the diagram expressing the mixed coassociativity condition:

$$\begin{aligned} (\text{id}_R \otimes c) (\partial(r)) &= (\text{id}_R \otimes c) \left(\sum_i \partial_i(r) \otimes \varepsilon^i \right) \\ &= \sum_i \partial_i(r) \otimes \left(\sum_{k=0}^i \binom{i}{k} \varepsilon^k \otimes \varepsilon^{i-k} \right) \\ &= \sum_{k+j < p^n} \binom{k+j}{k} \partial_{k+j} \otimes \varepsilon^k \otimes \varepsilon^j. \end{aligned}$$

Now, we “travel right and up” in the diagram expressing the mixed coassociativity condition:

$$\begin{aligned} (\partial \otimes \text{id}_{k[\varepsilon]}) (\partial(r)) &= (\partial \otimes \text{id}_{k[\varepsilon]}) \left(\sum_j \partial_j(r) \otimes \varepsilon^j \right) \\ &= \sum_j \left(\sum_k \partial_k (\partial_j(r)) \otimes \varepsilon^k \right) \otimes \varepsilon^j \\ &= \sum_{k,j} \partial_k (\partial_j(r)) \otimes \varepsilon^k \otimes \varepsilon^j. \end{aligned}$$

The conclusion is that a \mathbb{F}_p -algebra map $\partial : R \rightarrow R \otimes_{\mathbb{F}_p} \mathbb{F}_p[\varepsilon]$ satisfies the mixed coassociativity condition if and only if for each $i, j < p^n$ we have:

$$\partial_i \circ \partial_j = \binom{i+j}{i} \partial_{i+j},$$

where the right-hand side is understood as 0 in the case when $i+j \geq p^n$ (in such a case we also have that $p \mid \binom{i+j}{i}$).

Such a sequence $(\partial_i)_{i < p^n}$ as above (that is: corresponding to an action of the group scheme α_{p^n}) is sometimes called a *truncated iterative Hasse-Schmidt derivation* on R .

Remark 12.9. By Problem 11.3, actions of α_p on $\text{Spec}(R)$ correspond to derivations ∂ on R such that $\partial^{(p)} = 0$ (p -th compositional power).

For completeness, we mention below the “proper” (that is: non-truncated) case.

Definition 12.10. Let R be a ring.

- (1) A *Hasse-Schmidt derivation* on R is a sequence of maps $(\partial_n : R \rightarrow R)_{n \in \mathbb{N}}$ such that for all $x, y \in R$ and for all $n \in \mathbb{N}$, we have the following:
 - $\partial_0 = \text{id}_R$;
 - $\partial_n(x+y) = \partial_n(x) + \partial_n(y)$;
 - $\partial_n(xy) = \sum_{i+j=n} \partial_i(x) \partial_j(y)$ (“higher Leibniz rules”).
- (2) A *Hasse-Schmidt derivation* $(\partial_n : R \rightarrow R)_{n \in \mathbb{N}}$ on R is called *iterative*, if for all $m, n \in \mathbb{N}$ we have:

$$\partial_n \circ \partial_m = \binom{n+m}{m} \partial_{n+m}.$$

Remark 12.11. Two comments about Hasse-Schmidt derivations, which are only loosely related with the main topic of this lecture.

- (1) By Problem 11.5, if R is a \mathbb{Q} -algebra, then an iterative Hasse-Schmidt derivation on R is “the same” as a usual derivation. But in the case of positive characteristic these two notions differ and the notion of an iterative Hasse-Schmidt derivation is considered as a “better” one, the intuition being that we “improve” the compositional powers of the usual derivation ∂_1 .
- (2) In the case of positive prime characteristic p , an iterative Hasse-Schmidt derivation on R can be understood as a *compatible sequence* of actions of the finite group schemes $(\alpha_{p^n})_{n > 0}$. In the general case, there is only an interpretation as an action of a certain *formal group scheme* (not a group scheme!), which we will not explain here.

Problem List 11

Let k and K be fields, p be a prime number, and $n \in \mathbb{N}_{>0}$.

(1) Let A be a finite set.

(a) For any category \mathcal{C} , define properly the *constant functor*:

$$\text{Const}_A : \mathcal{C} \longrightarrow \mathbf{Sets}, \quad \text{Const}_A(X) = A.$$

(b) Show that for a *connected* (that is: 0 and 1 are the only idempotent elements) k -algebra R , we have the following bijection:

$$\text{Hom}_{\mathbf{Alg}_k}(k^A, R) \leftrightarrow A.$$

(c) Let \mathbf{Conn}_k denote the full subcategory of \mathbf{Alg}_k whose objects are connected k -algebras. Show that the following two functors are isomorphic:

$$h_{k^A} : \mathbf{Conn}_k \longrightarrow \mathbf{Sets}, \quad \text{Const}_A : \mathbf{Conn}_k \longrightarrow \mathbf{Sets}.$$

(2) Show that if X and Y are finite sets, then we have the following k -algebra isomorphism:

$$k^{X \times Y} \cong_k k^X \otimes_k k^Y.$$

(3) Assume that $\text{char}(R) = p$ and ∂ is a derivation on R . Show that $\partial^{(p)}$ (the p -th compositional power of ∂) is a derivation on R as well.

(4) Find a natural bijection between the set of actions of α_p on $\text{Spec}(R)$ and the set of k -derivation ∂ on R such that $\partial^{(p)} = 0$.

(5) Let $R \in \mathbf{Alg}_{\mathbb{Q}}$. Find a natural bijection between the set of iterative Hasse-Schmidt derivations on R and the set of derivations on R .

(6) Show that there is the following commutative diagram, where each row is exact, each column is exact, and $\mu_n(K) = \{x \in K^* \mid x^n = 1\}$:

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \mu_n(K) & \xrightarrow{\leq} & K^* & \xrightarrow{x \mapsto x^n} & (K^*)^n & \longrightarrow & 1 \\
 & & \downarrow x \mapsto xI & & \downarrow x \mapsto xI & & \downarrow \leq & & \\
 1 & \longrightarrow & \text{SL}_n(K) & \xrightarrow{\leq} & \text{GL}_n(K) & \xrightarrow{\det} & K^* & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 1 & \longrightarrow & \text{PSL}_n(K) & \longrightarrow & \text{PGL}_n(K) & \longrightarrow & K^*/(K^*)^n & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
 \end{array}$$

13. ACTIONS OF FINITE GROUP SCHEMES: MODEL THEORETICAL SET-UP

In today's lecture, we introduce a proper language for the theory of actions on fields of a fixed finite group scheme. We also start discussing a motivating example of the theory existentially closed differential fields in characteristic zero.

13.1. Actions of finite group schemes: language and theory. Let us fix the following:

- a field k ;
- a finite group scheme $\mathfrak{g} = \text{Spec}(H)$ over k ;
- $m := \dim_k H$;
- a k -basis $\{b_1, \dots, b_m\}$ of H over k ;
- a k -algebra R .

Any map $\partial : R \rightarrow R \otimes_k H$ corresponds to a sequence of maps $(\partial_i : R \rightarrow R)_{i \leq m}$ such that:

$$\partial(r) = \sum_{i=1}^m \partial_i(r) \otimes b_i.$$

A map $\partial : R \rightarrow R \otimes_k H$ is a coaction of H on R (equivalently: an action of \mathfrak{g} on $\text{Spec}(R)$) if and only if $\partial_1, \dots, \partial_m$ satisfy:

- additivity and “Leibniz rules” corresponding to ∂ being a k -algebra homomorphism;
- “iterativity rules” corresponding to ∂ satisfying the coaction conditions.

Example 13.1. We consider two main examples.

- (1) Suppose that $\mathfrak{g} = \text{Spec}(k^G)$.
 - Additivity and the “Leibniz rules” correspond to ∂_g being a \mathbf{k} -algebra endomorphism for $g \in G$.
 - The “iterativity rules” correspond to $\partial_e = \text{id}$ and $\partial_g \circ \partial_h = \partial_{gh}$ for each $g, h \in G$ (the group action axioms).
- (2) Suppose that $\mathfrak{g} = \alpha_{p^n}$ (kernel of Fr^n , see Example 12.3(2)).
 - Then, the “Leibniz rules” correspond to the actual (higher) Leibniz rules:

$$\partial_i(xy) = \sum_{j+l=i} \partial_j(x) \partial_l(y).$$

- The “Iterativity rules” correspond to the condition $\partial_0 = \text{id}$ and to the actual iterativity rules from the definition of an iterative (truncated) Hasse-Schmidt derivation:

$$\partial_i \circ \partial_j = \binom{i+j}{i} \partial_{i+j}.$$

The above conditions on $\partial_1, \dots, \partial_m$ saying that ∂ is an action of \mathfrak{g} on $\text{Spec}(R)$ can be expressed by a collection of sentences in the language of \mathfrak{g} -actions ($\partial_1, \dots, \partial_m$ are unary function symbols and $c \in k$ stand for constant symbols):

$$L_{\mathfrak{g}} := L_{\text{rings}} \cup \{\partial_1, \dots, \partial_m\} \cup \{c \mid c \in k\}.$$

The particular names for the unary function symbols $\partial_1, \dots, \partial_m$ may differ depending on the context. The above sentences can be written down by using the structure constants (see Definition 12.4) introduced during the previous lecture, but we will not write these sentences explicitly. We get the $L_{\mathfrak{g}}$ -theory \mathfrak{g} -DF, whose models are exactly fields with \mathfrak{g} -actions. We will use the obvious terminology of \mathfrak{g} -rings, \mathfrak{g} -fields, \mathfrak{g} -field (ring) extensions, etc.

Example 13.2. We consider two main examples again.

- (1) Suppose that $\mathfrak{g} = \text{Spec}(k^G)$. Then, the language $L_{\mathfrak{g}}$ coincides with the language L_G and the theory \mathfrak{g} -DF coincides with the theory G -TF (see Section 2.2).
- (2) Suppose that $\mathfrak{g} = \alpha_{p^n}$ (kernel of Fr^n). Then, in the language $L_{\mathfrak{g}}$ we have the unary function symbols $\partial_0, \dots, \partial_{p^n-1}$ and the theory $L_{\mathfrak{g}}$ says the following.
 - For each i , the map ∂_i is additive maps and for all $x, y \in R$, we have:

$$\partial_i(xy) = \sum_{j+l=i} \partial_j(x)\partial_l(y).$$

- $\partial_0 = \text{id}$.
- For each $i, j < p^n$ we have:

$$\partial_i \circ \partial_j = \binom{i+j}{i} \partial_{i+j},$$

where for $i+j \geq p^n$, the right-hand side is understood as 0.

13.2. The theory of existentially closed differential fields. By a *differential field*, we mean a pair (K, ∂) , where K is a field and ∂ is a derivation. Similarly, for a *differential ring* (commutative and with 1). We consider the theory of differential fields of characteristic 0, called DF_0 . The positive characteristic case will be discussed briefly later (see Remark 13.6).

Before the next theorem we need the following.

Definition 13.3. Let (R, ∂) be a differential ring and X be a variable (of length one).

- (1) Then,

$$R\{X\} := R[X, X', X'', \dots, X^{(i)}, \dots]$$

denotes the polynomial ring over R in infinitely many variables $(X^{(i)})_{i \in \mathbb{N}}$, where we use the following convention:

$$X^{(0)} := X, X^{(1)} := X', X^{(2)} := X'', \dots$$

- (2) The elements of $R\{X\}$ are called *differential polynomials* over R .
- (3) If $f \in R\{X\} \setminus R$, then there is a smallest $i \in \mathbb{N}$ such that

$$f \in R[X, X', \dots, X^{(i)}] \setminus R[X, X', X'', \dots, X^{(i-1)}]$$

(setting $R[X^{(-1)}] := R$). We call i as above the *order* of f . For $f \in R \setminus \{0\}$, the order of f is -1 and the zero polynomial does not have an order.

Remark 13.4. For the definition of the ring $R\{X\}$ above, we did not need to assume that there is a derivation on R . However, it is crucial that $R\{X\}$ becomes a differential ring, which we explain below. Let (R, ∂) be a differential ring.

- (1) There is a unique derivation ∂' on $R\{X\}$ such that for all $i \in \mathbb{N}$ we have

$$\partial \left(X^{(i)} \right) = X^{(i+1)}, \quad \partial'|_R = \partial.$$

- (2) For any $f \in R\{X\}$ and any $a \in R$, there is the obvious notion of the differential evaluation $f(a) \in R$.
- (3) For a fixed $a \in R$, the differential evaluation is a differential map, that is for all $f \in R\{X\}$ and $a \in R$, we have:

$$\partial(f(a)) = \partial'(f)(a).$$

Theorem 13.5 (Blum, 1968). *The theory DF_0 has a model companion, called DCF_0 , which has the following axioms: for each $f, g \in K\{X\} \setminus \{0\}$ such that the order of f is greater than the order of g , there is $a \in K$ such that $f(a) = 0$ and $g(a) \neq 0$.*

The notion of a differentially closed field was studied first by Robinson in 1950s. The theory DCF_0 is ω -stable of infinite rank and it is a very interesting theory (Zilber's trichotomy, relations between modular/trivial types and the corresponding differential equations, diophantine applications, etc.). In the next semester, I plan to organize a research seminar, where we will read the following recent paper, which uses the model theory of differential fields to prove new results in diophantine geometry and also to "give a complete proof of an assertion of Painlevé (1895)":

Guy Casale, James Freitag, Joel Nagloo, "Ax-Lindemann-Weierstrass with derivatives and the genus 0 Fuchsian groups", *Annals of Mathematics*, 721–765, Volume 192 (2020).

Remark 13.6. In the case of positive characteristic $p > 0$, Wood gave axioms of the theory DCF_p , which is a model companion of the theory of differential fields of characteristic p . There is one more condition in Wood's axioms corresponding to separability.

The theory DCF_p is strictly stable (in particular: it is *not* ω -stable) and it was studied by Shelah, Wood, and others in 1970s. Model-theoretically, it is still quite a mysterious theory (for example: Zilber's trichotomy is unknown), but it does not seem to have geometric applications (yet?).

14. GEOMETRIC AXIOMS IN DIFFERENTIAL CONTEXT

Our aim is to show that for any finite group scheme \mathfrak{g} , the theory \mathfrak{g} -DF has a model companion, which will generalize the corresponding result for finite groups (see Theorem 8.4). We start from a motivating example of the theory DCF_0 .

We are aiming to describe geometric axioms of the theory DCF_0 . We need a classical notion of the *tangent bundle* and a less classical one of the *twisted tangent bundle*. Let K be an algebraically closed field and $V \subseteq \mathbb{A}^n$ be a K -variety. If we have:

$$I(V) = (f_1, \dots, f_m) \trianglelefteq K[X_1, \dots, X_n],$$

then the ideal:

$$(f_1, \dots, f_m, f'_1, \dots, f'_m) \trianglelefteq K[X_1, \dots, X_n, X'_1, \dots, X'_n]$$

defines $TV \subseteq \mathbb{A}^{2n}$, the *tangent bundle* to V , where for $f \in K[X_1, \dots, X_n]$ we have:

$$f' := \sum_{i=1}^n \frac{\partial f}{\partial X_i} X'_i.$$

We include now several comments about the connections between the tangent bundle and the notion of smoothness. They are not related to our main topic of the geometric axiomatization, but they are still important.

Problem 12.1

The projection map $\mathbb{A}^{2n} \rightarrow \mathbb{A}^n$ induces a map $TV \rightarrow V$ whose fibers, denoted $T_v V$ and called *tangent spaces* (to V at v), have a natural structure of a vector space over K .

A variety V is *smooth* if and only if for all $v \in V$ all the tangent spaces $T_v V$ have the same dimension as K -vector spaces. We include a side remark below.

Remark 14.1. In the smooth case, this common dimension of tangent spaces above coincides with the *dimension of V* , which can be defined in terms of the Zariski topology on V and it also coincides with:

- the Krull dimension of the ring $K[V]$;
- for an irreducible V , the transcendence degree of the field $K(V)$ over K ;
- the Morley rank of V considered as a definable set in the field K ;
- the U -rank of V considered as a definable set in the field K .

In the context of DCF_0 , all these four dimension notions above make sense and they are all pairwise different!

If $K = \mathbb{C}$ and V is smooth, then V has a natural structure of a *differential manifold* (or even of a *complex manifold*) and the tangent bundle coincides with the one we know from differential geometry. Formally, there is a forgetful functor from the category of smooth algebraic \mathbb{C} -varieties to the category of differential manifolds (or to the category complex manifolds) and this forgetful functor commutes with the appropriate tangent bundle functors.

For any ring R , we consider:

$$R[\varepsilon] := R[X]/(X^2),$$

which is called the *ring of dual numbers*. The crucial property of the ring of dual numbers is that any homomorphism $R \rightarrow S[\varepsilon]$ is the same as a pair of maps $\sigma, \partial : R \rightarrow R$ (by the rule $r \mapsto \sigma(r) + \partial(r)\varepsilon$) such that σ is a ring homomorphism and ∂ is an additive map satisfying the following “ σ -Leibniz” multiplicative rule:

$$\partial(xy) = \sigma(x)\partial(y) + \sigma(y)\partial(x).$$

Definition 14.2. Let $\sigma : R \rightarrow T$ be a ring homomorphism. We call a map $\partial : R \rightarrow T$ a *derivation* of σ , if ∂ is additive and for all $x, y \in R$, we have:

$$\partial(xy) = \sigma(x)\partial(y) + \sigma(y)\partial(x).$$

In particular, derivations on R correspond to ring homomorphisms $\varphi : R \rightarrow R[\varepsilon]$ such that $\pi \circ \varphi = \text{id}_R$, where $\pi : R[\varepsilon] \rightarrow R$ is the projection homomorphism given by $\pi(r + r'\varepsilon) = r$.

Remark 14.3. We take now $R = \mathbb{R}$ and present some historical comments (Wikipedia).

- (1) The field of complex numbers $\mathbb{C} = \mathbb{R}[i]$ was introduced in the 16th century(?). The rule is $i^2 = -1$.
- (2) The ring of *split complex numbers* $\mathbb{R}[j]$ was introduced around 1848. The rule is $j^2 = 1$ (so, it is isomorphic with the ring $\mathbb{R} \times \mathbb{R}$, but the norm is different and somehow the norm matters).
- (3) The ring of dual numbers $\mathbb{R}[\varepsilon]$ was introduced by Clifford in 1873. The rule is $\varepsilon^2 = 0$.

Let us assume for simplicity that:

$$K[V] = K[X_1, \dots, X_n]/(f)$$

(so, V is a *hypersurface*) and we set:

$$X := (X_1, \dots, X_n), \quad X' := (X'_1, \dots, X'_n).$$

Let R be a K -algebra.

Lemma 14.4. *There is the following natural correspondence:*

$$\text{Hom}_{\mathbf{Alg}_K}(K[TV], R) \longleftrightarrow \text{Hom}_{\mathbf{Alg}_K}(K[V], R[\varepsilon]).$$

Proof. Let us take a K -algebra map:

$$f : K[V] \longrightarrow R[\varepsilon].$$

For any $i \leq n$, we define $r_i, r'_i \in R$ by the following formula:

$$f(X_i + (f)) = r_i + r'_i\varepsilon.$$

We define the following K -algebra map:

$$K[X, X'] \longrightarrow R, \quad X_i \mapsto r_i, \quad X'_i \mapsto r'_i.$$

It is easy to see that this map factors through $K[TV]$, so it induces a K -algebra map

$$f^\dagger : K[TV] \longrightarrow R.$$

It can be also easily checked that the “big” map:

$$\text{Hom}_{\mathbf{Alg}_K}(K[V], R[\varepsilon]) \ni f \mapsto f^\dagger \in \text{Hom}_{\mathbf{Alg}_K}(K[TV], R)$$

is a natural bijection. □

Remark 14.5. The above lemma has several interpretations which may clarify the notion of an algebraic tangent bundle.

- (1) By Problem 10.3, for any K -algebra R we have:

$$TV(R) = V(R[\varepsilon]).$$

- (2) In particular, the morphisms $V \rightarrow TV$, which are sections of the projection map $TV \rightarrow V$ (so, they are the classical *sections* of TV) correspond to K -derivations of $K[V]$, since we have:

$$\mathrm{Hom}_{\mathbf{AfVar}_K}(V, TV) = \mathrm{Hom}_{\mathbf{Alg}_K}(K[TV], K[V]) = \mathrm{Hom}_{\mathbf{Alg}_K}(K[V], K[V][\varepsilon]).$$

The following theorem extends Lemma 14.4 and Remark 14.5(1).

Theorem 14.6. *There is a functor:*

$$\mathcal{T} : \mathbf{Alg}_K \longrightarrow \mathbf{Alg}_K,$$

which has the following properties.

- (1) *For all $R, S \in \mathbf{Alg}_K$, we have the following natural bijection:*

$$\mathrm{Hom}_{\mathbf{Alg}_K}(\mathcal{T}(S), R) \longleftrightarrow \mathrm{Hom}_{\mathbf{Alg}_K}(S, R[\varepsilon]).$$

- (2) *For any $V \in \mathbf{AfVar}_K$, we have:*

$$\mathcal{T}(K[V]) = K[TV].$$

Proof. It follows as in the proof of Lemma 14.4. □

Remark 14.7. For all $R \in \mathbf{Alg}_K$, we have:

$$\mathcal{T}(R) = S(\Omega_{R/K}),$$

where $\Omega_{R/K}$ is the R -module of *Kähler differentials* and for any R -module M , $S(M)$ is the *symmetric algebra*.

The crucial categorical property of the functor \mathcal{T} from Theorem 14.6(1) is called *adjointness*. The general definition is below.

Definition 14.8. Let \mathcal{C} and \mathcal{D} be categories and

$$\mathcal{L} : \mathcal{C} \rightarrow \mathcal{D}, \quad \mathcal{R} : \mathcal{D} \rightarrow \mathcal{C}$$

be functors. The functor \mathcal{L} is *left-adjoint* to the functor \mathcal{R} (or \mathcal{R} is *right-adjoint* to \mathcal{L}), if the following functors are isomorphic

$$\mathcal{C}^{\mathrm{op}} \times \mathcal{D} \ni (X, Y) \mapsto \mathrm{Hom}_{\mathcal{D}}(\mathcal{L}(X), Y) \in \mathbf{Set};$$

$$\mathcal{C}^{\mathrm{op}} \times \mathcal{D} \ni (X, Y) \mapsto \mathrm{Hom}_{\mathcal{C}}(X, \mathcal{R}(Y)) \in \mathbf{Set}.$$

That is: for any $X \in \mathcal{C}, Y \in \mathcal{D}$, we have the following natural bijection:

$$\mathrm{Hom}_{\mathcal{D}}(\mathcal{L}(X), Y) \longleftrightarrow \mathrm{Hom}_{\mathcal{C}}(X, \mathcal{R}(Y)).$$

Example 14.9. Adjoint functors appear naturally in our mathematical life, we give some examples below.

- (1) Let \mathcal{R} be a forgetful functor. Then, a left-adjoint functor \mathcal{L} (if it exists) gives rise to “free objects”. We see some examples below.

(a) Let $\mathcal{R} : \mathbf{Grp} \rightarrow \mathbf{Set}$. Then, we get the *free group* functor:

$$\mathcal{L}(X) = F_X.$$

(b) Let $\mathcal{R} : \mathbf{Ab} \rightarrow \mathbf{Grp}$. Then, we get the *abelianization* functor:

$$\mathcal{L}(H) = H^{\text{ab}} = H/[H, H].$$

(c) Let S be an R -algebra and $\mathcal{R} : \mathbf{Mod}_S \rightarrow \mathbf{Mod}_R$ (this forgetful functor is also called the *restriction of scalars* functor). Then, we get the *extension of scalars* functor:

$$\mathcal{L}(M) = M \otimes_R S.$$

It works in the same way on the level of algebras, where $\mathcal{R} : \mathbf{Alg}_S \rightarrow \mathbf{Alg}_R$, which can be generalized to any category with products/coproducts (in place of the category of rings) and get the restriction/extension (of the base object) adjointness.

(d) Let $\mathcal{R} : \mathbf{Field} \rightarrow \mathbf{Domain}$. Then, we get the *fraction field* functor:

$$\mathcal{R}(R) = R_0$$

(we consider only ring monomorphisms as morphisms in the category **Domain**).

(2) For $(X, x) \in \mathbf{Top}_*$ let

$$\Omega(X, x) = \text{Hom}_{\mathbf{Top}_*}((S^1, *), (X, x))$$

(loops at x) with the compact-open topology.

$$\Sigma(X, x) = X \times [0, 1] / (X \times \{0, 1\} \cup \{x\} \times [0, 1])$$

(distinguished point for $\Omega(X, x)$ is the constant loop and for $\Sigma(X, x)$, it is $(x, 0)$).

Σ is left-adjoint to Ω , where Σ and Ω are functors from \mathbf{Top}_* to \mathbf{Top}_* .

(3) For a commutative ring R and an R -module M , the functor

$$\mathbf{Mod}_R \ni N \mapsto M \otimes_R N \in \mathbf{Mod}_R$$

is left-adjoint to the corresponding representable functor:

$$\mathbf{Mod}_R \ni N \mapsto h_M(N) = \text{Hom}_{\mathbf{Mod}_R}(M, N) \in \mathbf{Mod}_R.$$

(4) Let S be an R -algebra. We know that the extension of scalars functor:

$$\mathbf{Alg}_R \ni T \mapsto T \otimes_R S \in \mathbf{Alg}_S$$

has a right-adjoint which is the restriction of scalars functor. If S is free and finitely generated as an R -module, then the above extension of scalars functor has also a *left-adjoint* functor, which is called *Weil restriction*.

(5) In any category \mathcal{C} with products and coproducts, the functor

$$\mathcal{C} \ni X \mapsto X \coprod X \in \mathcal{C}$$

is left-adjoint to the functor

$$\mathcal{C} \ni X \mapsto X \times X \in \mathcal{C}.$$

Before finally getting to the geometric axioms of DCF_0 , let us recall the axioms of ACFA. Let (K, σ) be a field with an automorphism. For simplicity, we assume that the field K is algebraically closed. If $V = Z(I)$ is a variety given by the ideal $I \trianglelefteq K[X_1, \dots, X_n]$, then by ${}^\sigma V$ we denote the variety given by the ideal $\sigma(I)$ (σ acting on the coefficients of polynomials). We have the bijection map:

$$\sigma^{\times n} : K^n \longrightarrow K^n,$$

which induces the following bijection

$$\sigma_V := \sigma^{\times n}|_V : V \longrightarrow {}^\sigma V.$$

Axioms of ACFA

For any pair of irreducible varieties (V, W) , IF

- $W \subseteq V \times {}^\sigma V$,
- the projection maps:

$$W \longrightarrow V, \quad W \longrightarrow {}^\sigma V$$

are dominant (that is: the images are Zariski dense);

THEN there is $a \in V$ such that $(a, \sigma_V(a)) \in W$.

By Theorem 7.7, a difference field (K, σ) is existentially closed if and only if (K, σ) is a model of ACFA.

Suppose now that (K, ∂) is a differential field and V is a K -variety. For convenience we still assume that K is algebraically closed, since any existentially closed differential field of characteristic 0 is algebraically closed as a field. The role of $V \times {}^\sigma V$ from the axioms of ACFA is played by $T^\partial(V)$, which is a “twisted version” of the tangent bundle TV , similarly as $V \times {}^\sigma V$ is a “twisted version” of the Cartesian product $V \times V$. For $f \in K[X_1, \dots, X_n]$, we define:

$$\partial(f) := f^\partial + f',$$

where:

$$\left(\sum a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n} \right)^\partial := \sum \partial(a_{i_1 \dots i_n}) X_1^{i_1} \dots X_n^{i_n}.$$

Remark 14.10. The map

$$\partial : K[X_1, \dots, X_n] \longrightarrow K[X_1, \dots, X, X'_1, \dots, X'_n]$$

comes from the derivation on the ring of differential polynomials in n variables $K\{X_1, \dots, X_n\}$, which is defined in the similar way as in the case of a single variable.

We define the *twisted tangent bundle* to V , denoted $T^\partial(V)$, as the set of zeroes of:

$$(f_1, \dots, f_m, \partial(f_1), \dots, \partial(f_m)) \trianglelefteq K[X_1, \dots, X_n, X'_1, \dots, X'_n]$$

Problem 12.2

The map:

$$(\text{id}^{\times n}, \partial^{\times n}) : K^n \longrightarrow K^{2n}$$

induces the map

$$\partial_V := (\text{id}^{\times n}, \partial^{\times n})|_V : V(K) \longrightarrow T^\partial V(K).$$

Remark 14.11. The twisted tangent bundle $T^\partial V$ is a *torsor* of the tangent bundle TV , that is there is a morphism:

$$TV \times T^\partial V \longrightarrow T^\partial V$$

over V , which induces regular group actions of each $T_v V$ on $T_v^\partial V$.

More categorically, the tangent bundle TV is a *group in the category of varieties over V* and then the above map becomes an actual group action in this category.

We recall now that the ring of dual numbers “controls” derivation on R . Let us assume now that R is a K -algebra. We want to put a K -algebra structure on the ring $R[\varepsilon]$ such that this new K -algebra would control derivations on R extending the fixed derivation ∂ on K . Let us also denote by $\partial : K \rightarrow K[\varepsilon]$ the corresponding ring homomorphism. Let ∂' be a derivation on R and again we denote by the same symbol the following corresponding ring homomorphism: $\partial' : R \rightarrow R[\varepsilon]$. Let $\iota : K \rightarrow R$ denote the ring homomorphisms defining the K -algebra structure on R . Then, ∂' extends ∂ if and only if the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\partial'} & R[\varepsilon] \\ \iota \uparrow & & \uparrow \iota[\varepsilon] \\ K & \xrightarrow{\partial} & K[\varepsilon]. \end{array}$$

It is obvious now what is the right K -algebra structure on $R[\varepsilon]$ (the definition below).

Definition 14.12. By $R^\partial[\varepsilon]$, we denote the ring $R[\varepsilon]$ with the K -algebra structure given by the following composition:

$$K \xrightarrow{\partial} K[\varepsilon] \xrightarrow{\iota[\varepsilon]} R[\varepsilon].$$

It is clear now that the functor

$$\mathbf{Alg}_K \ni R \mapsto R^\partial[\varepsilon] \in \mathbf{Alg}_K$$

“controls” the derivations on R extending ∂ in the same way as the dual numbers functor “controlled” arbitrary derivations on R .

We also get the following version of Lemma 14.4.

Lemma 14.13. *There is the following natural correspondence:*

$$\mathrm{Hom}_{\mathbf{Alg}_K} (K[T^\partial V], R) \longleftrightarrow \mathrm{Hom}_{\mathbf{Alg}_K} (K[V], R^\partial[\varepsilon]).$$

We can finally formulate the following.

Geometric axioms of DCF_0

For any pair of irreducible varieties (V, W) , IF

- $W \subseteq T^\partial(V)$,
- the projection map $W \rightarrow V$ is dominant;

THEN there is $a \in V$ such that $\partial_V(a) \in W$.

Theorem 14.14 (Pierce-Pillay). *A differential field (K, ∂) of characteristic 0 is existentially closed if and only if (K, ∂) is a model of the geometric axioms of DCF_0 .*

Proof. For the left-to-right implication, we can assume as in the proof of Theorem 7.7 (since $W \rightarrow V$ is dominant) that:

$$V = \text{locus}_K(a), \quad W = \text{locus}_K(a, b)$$

for some tuples a, b in a (big) field extension M of K . Since we have $W \subseteq T^\partial V$, the inclusion $K[a] \rightarrow K[a, b]$ fits into the following commutative diagram:

$$\begin{array}{ccc} & & K[W] = K[a, b] \\ & \nearrow \subset & \uparrow \\ K[V] = K[a] & \longrightarrow & K[T^\partial V]. \end{array}$$

By Lemma 14.13, there is a canonical derivation of the map $K[V] \rightarrow K[T^\partial V]$ extending ∂ on K , which is adjoint to the identity map on $K[T^\partial V]$, since we have:

$$\text{Hom}_{\mathbf{Alg}_K}(K[V], K[T^\partial V][\varepsilon]) = \text{Hom}_{\mathbf{Alg}_K}(K[T^\partial V], K[T^\partial V]).$$

After composing with the map $K[T^\partial V] \rightarrow K[W]$, we get a derivation a derivation

$$\partial' : K[a] \rightarrow K[a, b]$$

of the inclusion $K[a] \rightarrow K[a, b]$ such that $\partial'(a) = b$ and ∂' extends ∂ . By Problem 12.3, ∂' extends to a derivation ∂'' of the field $K(a, b)$ and we can finish as in the proof of Theorem 7.7.

For the right-to-left implication, it is enough to repeat (after the appropriate changes) the corresponding part of the proof of Theorem 7.7. \square

Remark 14.15. We collect here several observations.

- (1) In the case of positive characteristic, the statement from Problem 12.3 is not true. For example, if ∂ is a derivation of the inclusion $\mathbb{F}_p(X^p) \subseteq \mathbb{F}_p(X)$ such that $\partial(X^p) \neq 0$, then ∂ cannot be extended to $\mathbb{F}_p(X)$.
- (2) The geometric axioms of ACFA and DCF_0 are very similar. The ambient varieties $V \times {}^\sigma V$ and $T^\partial V$ are different, but they fit into the same common general framework, which will be discussed during the last lecture.
- (3) To obtain the axioms of C_2 -TCF from the axioms of ACFA, one needs to include the “iterativity condition”:

$$\lambda_\sigma(W) = {}^\sigma W$$

and similarly for the theory G -TCF in the case of a finite group G .

- (4) In the next lecture, we will do something parallel to the passage from the axioms of ACFA to the axioms of C_2 -TCF discussed above. Namely, we will see what is the right “iterativity condition”, which needs to be added to the geometric axioms of DCF_0 to obtain the geometric axioms of α_2 -DCF, where α_2 is the finite group scheme being the kernel of the Frobenius map in characteristic 2.

Problem List 12

Let M be a field, K be an algebraically closed field, $V \subseteq \mathbb{A}^n$ be a variety, and $v \in V$.

- (1) Show that the projection map $\mathbb{A}^{2n} \rightarrow \mathbb{A}^n$ induces a map $TV \rightarrow V$ whose fibers have a natural structure of a vector space over K .
- (2) Assume that (K, ∂) is a differential field. Show that the map:

$$(\text{id}^{\times n}, \partial^{\times n}) : K^n \longrightarrow K^{2n}$$

induces the map

$$\partial_V := (\text{id}^{\times n}, \partial^{\times n})|_V : V(K) \longrightarrow T^\partial V(K).$$

- (3) Let $R \subseteq S$ be an extension of domains, M be the fraction field of S , and $\partial : R \rightarrow S$ be a derivation of the inclusion $R \subseteq S$. Show that ∂ extends to a derivation ∂' of M .
- (4) Assume that $\text{char}(M) = p$ and ∂ is a derivation on M s.t. $\partial^{(p^n)} = 0$. Show that

$$[M : \ker(\partial)] \leq p^n.$$

- (5) Assume that $(M, \partial) \models n - \text{DCF}_p$. Show the following.

- (a) The field M is separably closed.
- (b) $M^p = \ker(\partial)$.
- (c) $[M : M^p] = p^n$.

- (6) Show the following adjointness results.

- (a) The abelianization functor is left-adjoint to the forgetful functor

$$\mathcal{R} : \mathbf{Ab} \rightarrow \mathbf{Grp}.$$

- (b) Let S be an R -algebra. Then, the *extension of scalars* functor:

$$\mathcal{L}(M) = M \otimes_R S$$

is left-adjoint to the forgetful functor

$$\mathcal{R} : \mathbf{Mod}_S \rightarrow \mathbf{Mod}_R \quad (\text{or } \mathcal{R} : \mathbf{Alg}_S \rightarrow \mathbf{Alg}_R).$$

- (c) The *fraction field* functor is left-adjoint to the forgetful functor

$$\mathcal{R} : \mathbf{Field} \rightarrow \mathbf{Domain},$$

where morphisms in **Domain** are ring monomorphisms.

- (d) For a commutative ring R and an R -module M , the functor

$$\mathbf{Mod}_R \ni N \mapsto M \otimes_R N \in \mathbf{Mod}_R$$

is left-adjoint to the corresponding representable functor:

$$\mathbf{Mod}_R \ni N \mapsto h_M(N) = \text{Hom}_{\mathbf{Mod}_R}(M, N) \in \mathbf{Mod}_R.$$

- (e) In any category \mathcal{C} with products and coproducts, the functor

$$\mathcal{C} \ni X \mapsto X \coprod X \in \mathcal{C}$$

is left-adjoint to the functor

$$\mathcal{C} \ni X \mapsto X \times X \in \mathcal{C}.$$

- (f) Other examples you can think of.

15. THE THEORY \mathfrak{g} -DCF

Let us fix a field k and a finite group scheme \mathfrak{g} over k . In this final lecture, we will show that the theory \mathfrak{g} -DF has a model companion, which we call \mathfrak{g} -DCF, and we will briefly describe its model-theoretic properties. After having discussed the cases of G -TCF and the classical theories ACFA and DCF_0 , we still give one more particular example in the next subsection, before treating the general case. This particular example is a model companion of the theory of characteristic 2 fields with 2-nilpotent derivations.

15.1. The theory 1-DCF₂. We discuss now the theory α_2 -DF, which was considered first by Wood, who called it 1-DF. More generally, for any prime p and any $n > 0$, Wood considered the theory n -DF of fields of characteristic p with p^n -nilpotent derivations. For $n = 1$, this theory coincides (that is: it is bi-interpretable) with the theory α_p -DF (see Problem 11.4). Wood showed that a model companion of this theory exists and called it n -DCF. She did not specify the characteristic in the notation used for this theory, but, for clarity, we prefer to call these theories: n -DF _{p} and n -DCF _{p} .

Assume now that (K, ∂) is a differential field, $\text{char}(K) = 2$, and $\partial \circ \partial = 0$. We want to adapt the geometric axioms of DCF_0 to cover the differential fields as above in a similar manner as the axioms of ACFA were adapted to cover the case of G -actions, where G is a finite group.

Lemma 15.1. *Let V be K -variety. We have the following morphism:*

$$\lambda_V : T^\partial V \longrightarrow T^\partial (T^\partial V), \quad \lambda_V(v, v') = ((v, v'), (v', 0)).$$

Proof. We need to check that:

$$\lambda_{\mathbb{A}^n} (T^\partial V) \subseteq T^\partial (T^\partial V),$$

which is done on Figure 9. □

Such a choice of the morphism λ_V corresponds to the coordinate permutations, which were used in the case of the theory G -TCF. This choice will become clearer after the general finite group scheme interpretation.

Remark 15.2. Few comments about functorial properties of the morphism λ_V .

- (1) The morphism λ_V comes from the natural transformation

$$\lambda : T^\partial \longrightarrow T^\partial \circ T^\partial$$

or the following natural transformation

$$\lambda^\dagger : \mathcal{T}^\partial \circ \mathcal{T}^\partial \longrightarrow \mathcal{T}^\partial.$$

- (2) Any category of endofunctors becomes a *monoidal category* with the operation of composition of functors. In such a set-up, (T^∂, λ) is a *comonad* and $(\mathcal{T}^\partial, \lambda^\dagger)$ is a *monad*.
- (3) This last natural transformation λ^\dagger is not formally adjoint to λ , however it may be obtained by a very general argument, since it is well-known that adjointness takes monads to comonads and vice versa.
- (4) The notions of monad/comonad also appear in Computer Science, see e.g. <https://sonatsuer.github.io/monoid-homomorphisms-1.html> for a beginning of the story.

We are ready now to state the axioms.

Geometric axioms of 1 – DCF₂

For any pair of K -irreducible K -varieties (V, W) , IF

- $W \subseteq T^\partial(V)$,
- the projection map $W \rightarrow V$ is dominant,
- we have (the iterativity condition):

$$\lambda_V(W) \subseteq T^\partial(W);$$

THEN there is $a \in V(K)$ such that $\partial_V(a) \in W(K)$.

Theorem 15.3. *A differential field (K, ∂) of characteristic 2 such that $\partial \circ \partial = 0$ is existentially closed (in the class of such differential fields) if and only if (K, ∂) is a model of the geometric axioms of 1 – DCF₂.*

Proof. We sketch the proof which does not differ much from the proof in the general case. The morphism:

$$\lambda_V : T^\partial(V) \longrightarrow T^\partial(T^\partial V), \quad \lambda_V(v, v') = ((v, v'), (v', 0))$$

gives us the K -algebra map:

$$\lambda_V^* : K[T^\partial(T^\partial V)] \longrightarrow K[T^\partial V].$$

The adjoint map:

$$(\lambda_V^*)^\dagger : K[T^\partial V] \longrightarrow K[T^\partial V]^\partial[\varepsilon]$$

gives $K[T^\partial V]$ an α_2 -ring structure as before (coassociativity formally follows).

The iterativity condition implies that $K[W]$ gets the quotient α_2 -ring structure (induced from $K[T^\partial V]$) and afterwards the proof follows the lines of the G -TCF case (see the proof of Theorem 8.4). \square

15.2. Prolongations. In this subsection, we describe the main technical tool which is needed for the general case of the axioms of \mathfrak{g} -DCF. We will define the notion of a *prolongation* of a variety V , which will generalize the cases of $V \times {}^\sigma V$ and $T^\partial V$.

Recall that we have a functor:

$$\mathcal{T} : \mathbf{Alg}_K \longrightarrow \mathbf{Alg}_K$$

such that:

- for all $R, S \in \mathbf{Alg}_K$:

$$\mathrm{Hom}_{\mathbf{Alg}_K}(\mathcal{T}(S), R) \longleftarrow \mathrm{Hom}_{\mathbf{Alg}_K}(S, R[\varepsilon]).$$

- for any $V \in \mathbf{AfVar}_K$, we have:

$$\mathcal{T}(V) = K[TV].$$

Similarly, in the case of a differential field (K, ∂) , there is a functor:

$$\mathcal{T}^\partial : \mathbf{Alg}_K \longrightarrow \mathbf{Alg}_K$$

such that:

- for all $R, S \in \mathbf{Alg}_K$:

$$\mathrm{Hom}_{\mathbf{Alg}_K}(\mathcal{T}^\partial(S), R) \longleftarrow \mathrm{Hom}_{\mathbf{Alg}_K}(S, R^\partial[\varepsilon]).$$

- for any $V \in \mathbf{AfVar}_K$, we have:

$$\mathcal{T}^\partial(V) = K[T^\partial V].$$

Assume now that $\mathfrak{g} = \text{Spec}(H)$, where H is a Hopf algebra over k , which is finite-dimensional as a vector space over k . Assume that K is a \mathfrak{g} -field that is there is a coaction $\partial : K \rightarrow K \otimes_k H$ of H on K . We want to define a functor:

$$\mathbf{Alg}_K \longrightarrow \mathbf{Alg}_K,$$

which will “control” the extensions of ∂ to k -algebra maps $\partial' : R \rightarrow R \otimes_k H$ (coaction conditions are not important yet!) in a similar way as the twisted ring of dual numbers functor “controlled” the derivations on K -algebras extending a given derivation on K .

Definition 15.4. Let $R \in \mathbf{Alg}_K$. By $R \otimes_k^\partial H$, we denote the ring $R \otimes_k H$ with the K -algebra structure given by the following composition:

$$K \xrightarrow{\partial} K \otimes_k H \xrightarrow{\iota \otimes \text{id}_H} R \otimes_k H,$$

where $\iota : K \rightarrow R$ is the K -algebra structure map.

It is clear that the K -algebra $R \otimes_k^\partial H$ “controls” the extensions of ∂ to k -algebra maps $\partial' : R \rightarrow R \otimes_k H$.

We have the following general result. Instead of giving the proof, we only mention that the proof uses Weil restriction mentioned in Example 14.9(4) (left-adjoint to extension of scalars). The proof of the existence of Weil restriction is similar to the construction of the algebraic tangent bundle.

Theorem 15.5 (Moosa-Scanlon). *Let $k, \mathfrak{g}, K, \partial$ be as above.*

- (1) *There is a functor:*

$$\nabla^\partial : \mathbf{AfVar}_K \longrightarrow \mathbf{AfVar}_K$$

such that for all $V \in \mathbf{AfVar}_K$ and $R \in \mathbf{Alg}_K$, we have the following natural bijection:

$$\nabla^\partial V(R) \longleftrightarrow V(R \otimes_k^\partial H).$$

- (2) *We have a map (not coming from a morphism!):*

$$\partial_V : V(K) \longrightarrow \nabla^\partial V(K)$$

given on coordinates by

$$a \mapsto (\partial_1^{\times n}(a), \dots, \partial_m^{\times n}(a)),$$

where $V \subseteq \mathbb{A}^n$ and $m = \dim_k H$.

- (3) *There is a functor:*

$$\Delta_\partial : \mathbf{Alg}_K \longrightarrow \mathbf{Alg}_K,$$

which is left-adjoint to the functor $R \mapsto R \otimes_k^\partial H$ and such that for all $V \in \mathbf{AfVar}_K$ we have:

$$\Delta_\partial(K[V]) = K[\nabla^\partial V].$$

Example 15.6. Some particular examples of prolongations are below.

(1) If G is a finite group, $H = k^G$ and K is a G -field, then:

$$\nabla^\partial V = {}^G V = \prod_{g \in G} gV.$$

(2) If $\mathfrak{g} = \alpha_2$ and (K, ∂) is an α_2 -field, then:

$$\nabla^\partial V = T^\partial V.$$

(3) If $\mathfrak{g} = \alpha_{p^n}$ and (K, ∂) is an α_{p^n} -field, then $\nabla^\partial V$ is the “twisted p^n th arc space”, where arc spaces may be thought of as “higher tangent bundles” (some people also use the name “jet space” in this context).

So far, the Hopf algebra structure on H was not used. It is used for the proof of the following next result. We skip this proof, which is purely categorical.

Theorem 15.7. *There is a natural map:*

$$\lambda : \nabla^\partial \longrightarrow \nabla^\partial \circ \nabla^\partial$$

such that for all K -varieties V , the morphism

$$\lambda_V : \nabla^\partial V \longrightarrow \nabla^\partial (\nabla^\partial V)$$

induces a \mathfrak{g} -ring structure on $K[\nabla^\partial V]$.

Remark 15.8. (1) The comments from Remark 15.2 about monads/comonads apply also in this more general situation.

(2) The natural map λ_V may be given in coordinates using the structure constants of the cooperation on H (see Definition 12.4) in the following way:

$$\lambda_V(x_1, \dots, x_m) = \left(\sum_{l=1}^m c_l^{i,j} x_l \right)_{i,j < m},$$

where $m = \dim_k H$.

(3) In the particular case of $\mathfrak{g} = \alpha_2$, we see from Item (2) above that the formula for λ_V from Lemma 15.1 fits to the general case from Theorem 15.5.

15.3. Axiomatization and properties of \mathfrak{g} -DCF. We still have a fixed finite group scheme \mathfrak{g} over a field k . For any \mathfrak{g} -field (K, ∂) and a K -variety V , we also have the notion of a prolongation $\nabla^\partial V$ as in the previous subsection. We can finally state the axioms of a model companion of the theory \mathfrak{g} -DF, which was our aim for quite some time. They have exactly the same form as the geometric axioms for the theory α_2 -DCF discussed in Section 15.1.

Axioms of \mathfrak{g} -DCF

For any pair of K -irreducible K -varieties (V, W) , IF

- $W \subseteq \nabla^\partial(V)$,
- the projection map $W \rightarrow V$ is dominant,
- we have (the iterativity condition):

$$\lambda_V(W) \subseteq \nabla^\partial(W);$$

THEN there is $a \in V(K)$ such that $\partial_V(a) \in W(K)$.

The proof of the following main theorem is basically the same as the proof of Theorem 15.3 or the proof of Theorem 8.4 and we skip it.

Theorem 15.9. *A \mathfrak{g} -field (K, ∂) is existentially closed if and only if $(K, \partial) \models \mathfrak{g}\text{-DCF}$.*

Before presenting the model-theoretic properties of the theory $\mathfrak{g}\text{-DCF}$ (there will not be any time for proofs), we give some structural results about finite group schemes. These results also fit nicely into the (rather short) history of the model-theoretic approach to such actions.

It is a classical result that \mathfrak{g} fits into the following short exact sequence of finite group schemes:

$$1 \longrightarrow \mathfrak{g}^0 \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{g}_{\text{et}} \longrightarrow 1,$$

(it splits for a perfect k) where:

- (1) the finite group scheme \mathfrak{g}^0 is *connected*, that is: the corresponding Hopf algebra has no non-trivial idempotents;
- (2) the finite group scheme \mathfrak{g}_{et} is *étale*, that is: the corresponding Hopf algebra is *reduced* (no non-zero nilpotent elements).

Another classical result says that if $\text{char}(k) = 0$, then any connected finite group scheme is *trivial* (that is: it coincides with $\text{Spec}(k)$). In other words: if $\text{char}(k) = 0$, then the finite group scheme \mathfrak{g} is étale.

We know that the finite group scheme α_{p^n} is connected. The model theory of actions on fields of some types of connected group schemes was studied in the paper:

Hoffmann, Kowalski: “Existentially closed fields with G -derivations”, *Journal of the London Mathematical Society*.

Finite *constant group schemes* (i.e. those of the form $\text{Spec}(k^G)$) are étale. More generally, a finite group scheme is étale if and only if it is a constant group scheme after a base field extension $k \subseteq k'$.

Example 15.10. The finite group scheme (*3rd roots of unity* over reals):

$$\mu_{3,\mathbb{R}} : \mathbf{Alg}_{\mathbb{R}} \rightarrow \mathbf{Gps}, \quad \mu_{3,\mathbb{R}}(R) = \{r \in R \mid r^3 = 1\}$$

is étale and non-constant: it becomes the constant group scheme $\text{Spec}(\mathbb{C}^{C_3})$ after the base field extension $\mathbb{R} \subset \mathbb{C}$.

Actions of non-constant étale finite group schemes are a bit mysterious. The model theory of actions of finite groups (equivalently: of constant group schemes) on fields was studied in the paper:

Hoffmann, Kowalski: “Existentially closed fields with finite group actions”, *Journal of Mathematical Logic*.

The results about the theory $\mathfrak{g}\text{-DCF}$ generalizing the connected case and étale case are from the recent preprint:

Hoffmann, Kowalski: “Model theory of fields with finite group scheme actions”.

The main results of this last paper are listed below.

- (1) The theory \mathfrak{g} -DF has a model companion, which is denoted by \mathfrak{g} -DCF (discussed above).
- (2) The theory \mathfrak{g} -DCF is simple. If both \mathfrak{g}^0 and fg_{et} are non-trivial, then it is *strictly simple*, that is: simple, not stable, and not supersimple.
- (3) The theory of actions of a fixed finite group G on fields of fixed characteristic $p > 0$ and of finite imperfection degree e has a model companion, which is bi-interpretable (after adding finitely many constants) with the theory \mathfrak{g} -DCF, where:

$$\mathfrak{g} := \ker(\text{Fr}_{\mathbb{G}_a^e}) \times \text{Spec}\left((\mathbb{F}_p)^G\right).$$

If G is non-trivial, then this theory is strictly simple.

To finish the entire lecture, we briefly discuss Items (2) and (3) above.

Let (R, ∂) be a \mathfrak{g} -ring, so $\partial : R \rightarrow R \otimes_{\mathbf{k}} H$.

Definition 15.11. We denote by $R^{\mathfrak{g}}$ the *ring of constants* of (R, ∂) , that is:

$$R^{\mathfrak{g}} := \{r \in R \mid \partial(r) = r \otimes 1\}.$$

Example 15.12. We give two examples of rings of constants.

- If $\mathfrak{g} = \text{Spec}(k^G)$, then $R^{\mathfrak{g}} = R^G$.
- If $\mathfrak{g} = \alpha_p$, then

$$R^{\mathfrak{g}} = R^d := \{r \in R \mid d(r) = 0\} \supseteq R^p,$$

where $d = \partial_1$ is a p -nilpotent derivation on R defining ∂ .

Remark 15.13. We still assume that (R, ∂) is a \mathfrak{g} -ring.

- It is known that the ring extension $R^{\mathfrak{g}} \subseteq R$ is integral.
- The extension $R^{\mathfrak{g}} \subseteq R$ need *not* be finite, that is R is not necessarily a finitely generated $R^{\mathfrak{g}}$ -module.
- There is a Noetherian domain R with an action of the group C_2 such that R^{C_2} is not Noetherian and R is not a finite R^{C_2} -module.
- We showed that if $K = R$ is a field, then the field extension $K^{\mathfrak{g}} \subseteq K$ is finite and of degree bounded by $\dim_{\mathbf{k}} H$, as in the case of group actions. It is hard to believe that this result is new, but we were unable to find it in the literature.

Using the last result, we get (similarly as in the case of G -TCF) that each model of the theory \mathfrak{g} -DCF is bi-intepretable with the pure field of constants. Therefore, to show the simplicity of the theory \mathfrak{g} -DCF, it is enough to show the simplicity of the theory of the pure field of constants. This is done similarly as in the G -TFC case:

- first we show that the field of constants is PAC (relatively easy);
- then we show that it is bounded, which is enough for the simplicity by the known results about the model theory of PAC fields (boundedness is more difficult than in the G -TCF case, since the extension $K^{\mathfrak{g}} \subseteq K$ is often neither normal nor separable).

The above concludes the discussion about Item (2).

Regarding Item (3), let e be a positive integer, p be a prime, and $\text{SF}_{p,e}$ be the theory of fields of characteristic p and imperfection degree e , that is:

$$[K : K^p] = p^e.$$

Let G be a finite group and:

$$\mathfrak{g} := \ker(\text{Fr}_{\mathbb{G}_a^e}) \times \text{Spec}\left((\mathbb{F}_p)^G\right).$$

We showed the following.

Theorem 15.14. *After adding finitely many constants, the theory \mathfrak{g} -DF is bi-interpretable with the theory of actions of the group G on models of $\text{SF}_{p,e}$.*

The above theorem implies the following.

Corollary 15.15. *A model companion of the theory of actions of the group G on models of $\text{SF}_{p,e}$ exists, it is strictly simple and (after adding finitely many constants) it is bi-interpretable with the theory \mathfrak{g} -DCF.*

FIGURE 1.

\mathcal{C} : category, $X \in \mathcal{C}$

$h_x: \mathcal{C} \rightarrow \text{Set}$ $h_x(Y) = \text{Hom}(X, Y)$, $h^x: \mathcal{C}^{\text{op}} \rightarrow \text{Set}$ $h^x(Y) = \text{Hom}(Y, X)$.

How do the functors h_x, h^x act on morphisms? $Y, Z \in \mathcal{C}$

Let $f: Y \rightarrow Z$.

abstract composition in category \mathcal{C}

$$\text{Hom}(X, Y) \xrightarrow{h_x(f) = f_*} \text{Hom}(X, Z) = \text{Hom}(X, Z)$$

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ & \searrow & \downarrow f \\ & & Z \end{array} \quad \begin{array}{ccc} Y & \xrightarrow{f} & Z \\ & \searrow & \downarrow f' \\ & & Z' \end{array} \quad \text{in } \mathcal{C}$$

$$\text{Set} [\text{Hom}(X, Y) \xrightarrow{f_*} \text{Hom}(X, Z) \xrightarrow{f'_*} \text{Hom}(X, Z')]$$

$$(f'_* \circ f_*)(\varphi) = (f'_* \circ f_*) \circ \varphi \stackrel{\text{assoc.}}{=} f'_* \circ (f_* \circ \varphi) = f'_* \circ f_* (\varphi) = f'_* (f_* (\varphi)) =$$

$$= (f'_* \circ f_*)(\varphi) \implies (f'_* \circ f_*) = f'_* \circ f_* \quad \text{It means}$$

real composition of functions

$$\boxed{ \begin{array}{c} Y \xrightarrow{\text{id}_Y} Y \\ (\text{id}_Y)_*(\varphi) = \text{id}_Y \circ \varphi \\ \text{So } (\text{id}_Y)_* = \text{id}_{\text{Hom}(X, Y)} \end{array} } \quad h_x(f'_* \circ f_*) = h_x(f'_*) \circ h_x(f_*)$$

$$Y' \xrightarrow{f'} Y \xrightarrow{f} Z$$

$$h^x(Y) = \text{Hom}(Y, X) \xleftarrow{h^x(f) = f^*} \text{Hom}(Z, X) = h^x(Z) \ni \varphi: Z \rightarrow X$$

$$\begin{array}{ccc} Y & & \\ \downarrow f & \searrow & \\ Z & \xrightarrow{\varphi} & X \end{array} \quad \begin{array}{l} f^*(\varphi) = \varphi \circ f \\ (f \circ f')^* = (f')^* \circ f^* \end{array} \quad \text{With calculations as above, we get:}$$

FIGURE 2.

(G, \cdot) is a group.
 $h^G: \text{Set}^{\text{op}} \rightarrow \text{Set}$

$$h^G(Y) = \text{Hom}(Y, G) = \frac{\text{Functions}(Y, G)}{G^Y}$$

it has the following group structure.

$y \in Y$
 $\forall \varphi, \psi: Y \rightarrow G$

$$(\varphi \cdot \psi)(y) := \varphi(y) \cdot \psi(y)$$

group operation in G

How about
 $y \in Y \xrightarrow{f} Z$

morphisms?

$$\text{Hom}(Y, G) \xleftarrow{f^*} \text{Hom}(Z, G) \ni \varphi, \psi \quad f^*: \text{homom. of groups}$$

$f^*(\varphi) = \varphi \circ f$

$$\begin{aligned} [f^*(\varphi \cdot \psi)](y) &= [(\varphi \cdot \psi) \circ f](y) = (\varphi \cdot \psi)(f(y)) = \varphi(f(y)) \cdot \psi(f(y)) = \\ &= \underbrace{f^*(\varphi)(y)}_{\text{in } G} \cdot f^*(\psi)(y) = [f^*(\varphi) \cdot f^*(\psi)](y) \end{aligned}$$

So f^* is a homomorphism in G .

FIGURE 3.

(G, μ, e, i)
 group object in \mathcal{C} $Y \in \mathcal{C}$
 $h^G: \mathcal{C}^{op} \rightarrow \text{Set} \quad h^G(Y) = \underline{\text{Hom}_{\mathcal{C}}(Y, G)}$
 $\mu: G \times G \rightarrow G$

We will describe a natural group structure here.

$$\text{Hom}_{\mathcal{C}}(Y, G) \times \text{Hom}_{\mathcal{C}}(Y, G) \cong \underset{\uparrow}{\text{Hom}_{\mathcal{C}}(Y, G \times G)}$$

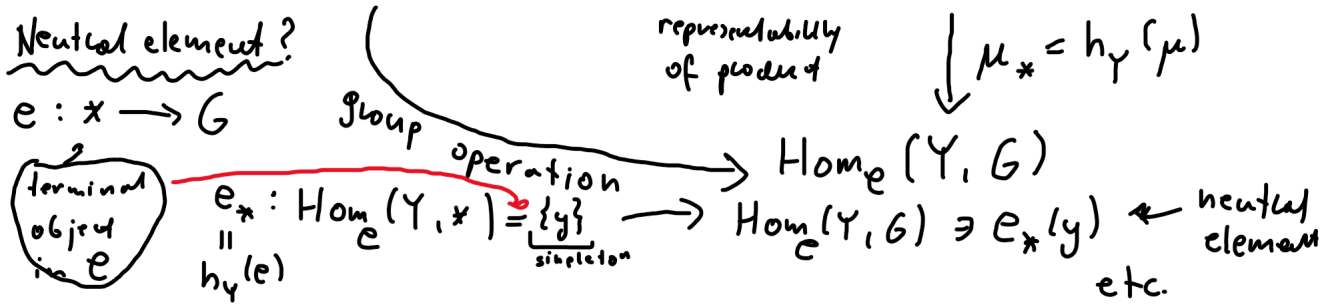


FIGURE 4.

$$\begin{aligned}
 + : A^2 = A^1 \times A^1 &\rightarrow A^1 & - : A^1 &\rightarrow A^1 & 0 : * &\rightarrow A^1 \\
 (a, b) &\mapsto a+b & a &\mapsto -a & \text{im}(0) &= \{0\}
 \end{aligned}$$

$$K[A^2] = K[x_1, x_2] \cong K[x] \otimes_K K[x], \quad K[A^1] = K[x], \quad K[*] = K$$

$x_1 \mapsto x \otimes 1$ $x_2 \mapsto 1 \otimes x$

$$+^* : K[A^1] \rightarrow K[A^2] = K[x_1, x_2] \cong K[x] \otimes K[x]$$

$f \in K[x] \quad +^*(f) = f \circ + \quad A^2 \xrightarrow{+} A^1 \xrightarrow{f} K$

$$+^*(f) = f(x_1 + x_2) \iff f(x \otimes 1 + 1 \otimes x)$$

$$+^* : K[x] \rightarrow K[x] \otimes K[x]$$

$x \mapsto x \otimes 1 + 1 \otimes x$

← Hopf algebra condition.

Hopf algebra structure on $K[x]$

$$\begin{array}{ccc}
 (x \otimes 1 + 1 \otimes x) \otimes 1 + (1 \otimes 1) \otimes x & \xleftarrow{\text{coassociativity diagram}} & x \otimes 1 + 1 \otimes x \\
 \parallel & & \\
 K[x] \otimes K[x] \otimes K[x] & \xleftarrow{+^* \otimes \text{id}} & K[x] \otimes K[x]
 \end{array}$$

$$\begin{array}{ccc}
 (x \otimes (1 \otimes 1) + 1 \otimes (x \otimes 1 + 1 \otimes x)) & \xleftarrow{\text{id} \otimes +^*} & K[x] \otimes K[x] \\
 & \xleftarrow{+^*} & K[x] \\
 & & \uparrow +^* \\
 & & K[x] \otimes K[x]
 \end{array}$$

↘ simpleton

$$\rightarrow^* : K[x] \rightarrow K[x]$$

$x \mapsto -x$

$$0^* : K[x] \rightarrow K[*] = K$$

$x \mapsto 0$

FIGURE 5.

$$C = Z(XY - 1)$$

$$K^* \longleftrightarrow C$$

$$x \longmapsto (x, x^{-1})$$

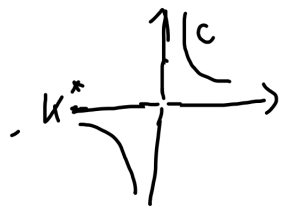
$$\mu: C \times C \longrightarrow C$$

$$((x_1, x_1^{-1}), (x_2, x_2^{-1})) \longmapsto (x_1 x_2, x_2^{-1} x_1^{-1})$$

$$i: C \longrightarrow C$$

$$(x, x^{-1}) \longmapsto (x^{-1}, x)$$

$$1: * \longrightarrow C$$

$$i_m(1) = \{(1, 1)\}$$


$$K[C] = K[X, Y] / (YX - 1) \cong K[X, 1/X]$$

$$x \mapsto X, \quad x^{-1} \mapsto 1/X$$

$$K[C \times C] \cong K[C] \otimes_K K[C] \cong K[X, 1/X] \otimes_K K[X, 1/X] \cong K[X_1, X_2, 1/X_1, 1/X_2]$$

$$\mu^*: K[C] \longrightarrow K[C \times C]$$

$$\mu^*(f) = f \circ \mu$$

$$C \times C \xrightarrow{\mu} C \xrightarrow{f} K$$

$$((x_1, x_1^{-1}), (x_2, x_2^{-1})) \xrightarrow{\mu} (x_1 x_2, x_2^{-1} x_1^{-1}) \xrightarrow{f} f(x_1 x_2, x_2^{-1} x_1^{-1})$$

$$\mu^*(f) = f(X_1 X_2, X_2^{-1} X_1^{-1}) \iff f(X \otimes X, 1/X \otimes 1/X)$$

$$\mu^*(x) = X \otimes X, \quad i^*(x) = X^{-1}, \quad 1^*(x) = 1.$$

FIGURE 6.

$$g, h, k \in G$$

$$\begin{array}{ccc}
 G \times G & \xrightarrow{\mu} & G \\
 \searrow \mu^*(\chi_g) & & \downarrow \chi_g \\
 & & k
 \end{array}$$

$$\chi_g(x) = \begin{cases} 1 & x=g \\ 0 & \text{ } \end{cases}$$

$$\mu^*(\chi_g)((h, k)) = \chi_g(\mu(h, k)) = \chi_g(hk) = \begin{cases} 1 & g=hk \\ 0 & \text{ } \end{cases}$$

$$\begin{array}{ccc}
 k^{G \times G} & \xrightarrow{\mu^*(\chi_g)} & \\
 \downarrow \cong & & \downarrow \\
 k^G \otimes_k k^G & & \sum_{hk=g} \chi_h \otimes \chi_k
 \end{array}$$

FIGURE 7.

$$\begin{array}{ccc}
 R \otimes_k G & \xrightarrow{id_R \otimes \mu^*} & R \otimes_k G \otimes_k G \\
 \uparrow \partial & & \uparrow \partial \otimes id_k \\
 r \in R & \xrightarrow{\partial} & R \otimes_k G
 \end{array}
 \quad \forall g \in G \quad \partial_g \in \text{Aut}_k(R)$$

$$\partial(r) = \sum_g \underbrace{\partial_g(r)} \otimes \chi_g$$

$$\sum_g \partial_g(r) \otimes \left(\sum_{hk=g} \chi_h \otimes \chi_k \right) \quad \Bigg| \quad \sum_g \left(\sum_h \partial_h(\partial_g(r)) \otimes \chi_h \right) \otimes \chi_g$$

$$\parallel \qquad \qquad \qquad \parallel$$

$$\sum_{h,k} \partial_{hk}(r) \otimes \chi_h \otimes \chi_k = \sum_{g,h} \partial_h(\partial_g(r)) \otimes \chi_h \otimes \chi_g$$

↑ mixed coassociativity of ∂
(g) \rightsquigarrow (k)

$$\forall h, k \in G \quad \partial_{hk} = \partial_h \circ \partial_k \quad \left(\begin{array}{l} \text{mixed associativity} \\ \text{of group action} \end{array} \right)$$

From the coaction $\partial: R \rightarrow R \otimes_k G$ of k^G on R
 we get k -alp. maps $(\partial_g: R \rightarrow R)_{g \in G}$
 giving a map $G \times R \xrightarrow{\Psi} R$
 $(g, r) \mapsto \partial_g(r)$

And the counit and mixed coassociativity conditions say exactly that Ψ is a group action (of G on R by k -algebra automorphisms).

FIGURE 8.

$$\partial: R \rightarrow R \otimes_{\mathbb{F}_p} \mathbb{F}_p[\varepsilon], \quad \mathbb{F}_p[\varepsilon] = \mathbb{F}_p[X] / (X^{p^n})$$

$$r, r' \in R, \quad \partial(r) = \sum_{i < p^n} \partial_i(r) \otimes \varepsilon^i.$$

$$\partial(r+r') = \sum_i \partial_i(r+r') \otimes \varepsilon^i$$

$$\partial(r) + \partial(r') = \sum_i \partial_i(r) \otimes \varepsilon^i + \sum_i \partial_i(r') \otimes \varepsilon^i = \sum_i (\partial_i(r) + \partial_i(r')) \otimes \varepsilon^i$$

$$\partial: \text{additive} \iff \forall i \quad \partial_i: \text{additive}$$

$$\partial(rr') = \sum_i \partial_i(rr') \otimes \varepsilon^i$$

$$\partial(r)\partial(r') = \left(\sum_j \partial_j(r) \otimes \varepsilon^j \right) \left(\sum_k \partial_k(r') \otimes \varepsilon^k \right)$$

$$= \sum_{j,k} \partial_j(r) \partial_k(r') \otimes \varepsilon^{j+k}$$

$$= \sum_i \left(\sum_{j+k=i} \partial_j(r) \partial_k(r') \right) \otimes \varepsilon^i$$

$$\partial: \text{multiplicative} \iff \forall i \quad \partial_i(rr') = \sum_{j+k=i} \partial_j(r) \partial_k(r')$$

FIGURE 9.

$$V \subseteq A^n$$

$$\lambda : (A^n)^2 \rightarrow (A^n)^4 \quad \lambda(v, v') = ((v, v'), (v', 0))$$

We have to check that if $V \subseteq A^n$, $\partial \circ \partial = 0$,
and $\text{char}(K) = 2$, then:

$$\lambda(T^2V) \subseteq T^2(T^2V) \quad (T^2V = Z(f, f^2 + f'))$$

For simplicity we assume that $V = Z(f)$ for

$f \in \ker(\partial)[X]$, so $T^2V = TV$ and $T^2(T^2V) = T(TV)$
(We'll discuss the general case $f \in K[X]$ which uses at the end.)

$$(v, v') \quad TV = Z(f, f') \quad , \quad T(T(v)) = Z(f, f', 'f, 'f') \quad , \quad \text{where}$$

$$\begin{matrix} \downarrow \\ (v, v'), (v', 0) \end{matrix} \quad K[X, X'] \rightarrow K[X, X', 'X, 'X']$$

$$\psi \mapsto ' \psi \quad X \mapsto 'X, X' \mapsto 'X' \quad \text{derivation}$$

$$\text{AIM: } 'f'(v, v'), (v', 0) \stackrel{?}{=} 0$$

$$f' = \sum_i \frac{\partial f}{\partial X_i} X_i'$$

$$'f' = \underbrace{\sum_i \left(\frac{\partial f}{\partial X_i} \right) X_i'} + \underbrace{\sum_i \frac{\partial f}{\partial X_i} 'X_i'}_{0 \text{ after evaluating at } ((v, v'), (v', 0))}$$

$$\parallel$$

$$\sum_i \left(\sum_j \frac{\partial^2 f}{\partial X_i \partial X_j} 'X_j \right) X_i' = \sum_{i,j} \frac{\partial^2 f}{\partial X_i \partial X_j} 'X_j X_i' =$$

$$= \sum_i \underbrace{\left[\frac{\partial^2 f}{\partial X_i \partial X_i} \right]}_{\substack{0 \text{ (char=2)} \\ ((X^n)' = n(n-1)X^{n-2} = 0)}} 'X_i X_i' + \sum_{i < j} \frac{\partial^2 f}{\partial X_i \partial X_j} \underbrace{('X_i X_j' + 'X_j X_i')}_{\substack{v_i' v_j' + v_j' v_i' = 0 \\ \text{after evaluating} \\ \text{OK.}}} .$$

General case

$$(f^2 + f')^2 + '(f^2 + f') = \underbrace{f^2}_{0 \text{ (char=2)}} + \underbrace{(f')^2 + '(f^2) + f'}_{0 \text{ on } (v, v'), (v', 0)}$$

→ since $(f^2)' = (f')^2$

0 after evaluated
(p.u.v.f above)