NUMBER THEORETICAL TOPICS IN INVERSE GALOIS THEORY

PIERRE DÈBES

Abstract. The aim of the course is to introduce the audience to inverse Galois theory and to some number theoretical topics involved in inverse Galois theory. We will set some recent result of the lecturer as the final goal and will use it as a motivation to discuss the topics that it goes through: the Inverse Galois problems, the geometric approach, Hilbert's irreducibility theorem, the Tchebotarev theorem, the Grunwald problem, the Malle conjecture, some diophantine material on curves: Lang-Weil over finite fields, Heath-Brown-Walkowiak over the rationals, etc.

The first four sections correspond to the three lectures while the last section corresponds to the research talk which will be the outcome of the course.

1. Inverse Galois theory

An introduction to the main questions from Inverse Galois theory that will enter in the course. In terms of field extensions, with a focus on the case that the base field is $\mathbb{Q}$ or a number field.

Main reference: [Dèb09, chapter 2]

1.1. **Arithmetic inverse Galois theory.** Inverse Galois Problem (IGP), the Grunwald problem, the Malle conjecture.

1.2. **Geometric inverse Galois theory.** Regular Galois extensions. Regular Inverse Galois problem (RIGP). Riemann's existence theorem. The descent question.

1.3. **Hilbert's irreducibility theorem (HIT).** Polynomial form. Specialized extension $F_{t_0}/\mathbb{Q}$ of $F/\mathbb{Q}(T)$ at t_0. RIGP $\Rightarrow$ IGP (no detailed proof at this point; in fact HIT and RIGP $\Rightarrow$ IGP are contained in the main result of the course and the method provides a proof of them).

Date: July 12, 2015.
2010 *Mathematics Subject Classification.* Primary ; Secondary .
Key words and phrases. Galois extensions, inverse Galois theory, ...

1.4. Problems around the specialization process.

Questions 1.1. *Does a regular Galois extension $F/k(T)$ of group G*

(a) *have a given Galois extension E/k of group $H \subset G$ among its unbranched specializations ?* (*Cf.* the twisting lemma and the Beckmann-Black problem).

(b) *have all Galois extensions E/k of group $H \subset G$ among its unbranched specializations ?* (*Cf.* parametric extensions).

(c) *have among its unbranched specializations a Galois extension E/k of group G with a specified local behavior at finitely many primes?* (*Cf.* the Grunwald problem).

(d) *have a specialization F_{t_0}/k of group G with t_0 "small" ? e.g. bounded in terms of the degree $[F:\mathbb{Q}(T)]$ and the genus g of F?* (*Cf.* effective HIT).

(e) *have many Galois extensions of group G among its unbranched specializations? with a bounded discriminant?* (*Cf.* the Malle conjecture).

Goal of the mini-course: provide answers to questions (a), (c), (d), (e) and discuss the implications to the related topics. Question (b) is discussed in François Legrand's papers.

Reference: [Dèb01]

Further bibliographic references: [FJ04], [Sch00], [Lan83]

2. The Hilbert-Grunwald theorem

Main reference: [DG12]

2.1. The function field Tchebotarev theorem.

Assume from now on that k is a number field and let $\mathcal{O}_k$ be its ring of integers.

Theorem 2.1. *Let $\mathfrak{p} \subset \mathcal{O}_k$ be a good prime of the k-regular Galois extension $F/k(T)$, of suitably large norm $N_{k/\mathbb{Q}}(\mathfrak{p})$. Let $\omega \in G\mathrm{Gal}(F/k(T)$. Then there exists an integer $t_\mathfrak{p} \in \mathbb{Z}$ such that for every $t_0 \in (\mathcal{O}_k)_\mathfrak{p}$ with $t_0 \equiv t_\mathfrak{p}$ modulo $\mathfrak{p}$, the Frobenius at $\mathfrak{p}$ of the specialized extension F_{t_0}/k is conjugate to ω in G.*

Reminder: the classical density Tchebotarev theorem.

2.2. From Tchebotarev to Hilbert-Grunwald.

Globalizing the previous result: Chinese remainder theorem, Jordan's lemma. Unramified Grunwald problem. Effectiveness.

2.3. **The Hilbert-Grunwald theorem.** Several forms will be given, including this one:

Corollary 2.2. *Given a regular Galois extension $F/\mathbb{Q}(T)$ of group G, there exist positive constant c_1 and c_2 (depending on $F/\mathbb{Q}(T)$) with the following property. For every $B > 0$, if $\mathcal{H}_B$ denotes the set of all $t_0 \in \mathbb{Z} \cap [1, B]$ such that* $\mathrm{Gal}(F_{t_0}/\mathbb{Q}) = G$*, then we have*

$$\mathrm{card}(\mathcal{H}_B) \geq \frac{c_1\, B}{c_2^{\log(B)/\log\log(B)}} \qquad (\text{for } B \gg 1)$$

3. The twisting lemma

Main references: [DG12], [DL12]

3.1. **Fundamental group representations.** [Dèb09, chapter 3] Discriminant, branch point set, fundamental groups

3.2. **Twisting fundamental group representations.** Definition, arithmetic and geometric interpretations, the twisting lemma.

3.3. **The Beckmann-Black problem over PAC fields.**

4. The function field Tchebotarev theorem

Main reference: [DG12]

4.1. **Grothendieck good reduction theorem.** Presentation without proof. References: [Gro71], [GM71].

4.2. **Lang-Weil estimates.** Presentation without proof.
Reference: [FJ04, chapters 4 & 5].

4.3. **Proof of the function field Tchebotarev theorem.**

5. Specialization results in Galois theory

5.1. **The Hilbert-Malle theorem.** A version of Hilbert's irreducibility theorem that counts not just the specialization points but the specialized extensions themselves.

5.2. **Main results.** Let G be a finite group of order $d \geq 2$ with a regular realization $F/\mathbb{Q}(T)$ and $P(T,Y) \in \mathbb{Z}[T,Y]$ be an affine model of $F/\mathbb{Q}(T)$ (the irreducible polynomial of a primitive element, integral over $\mathbb{Z}[T]$). Let ρ be the number of distinct roots of the discriminant $\Delta_P(T)$ of P w.r.t. to Y and $\mathcal{B}_P \in \mathbb{Z}$ the "bad prime divisor" of P.

Theorem 5.1. *If $p_1, \ldots, p_d$ are d distinct prime numbers $\geq \rho^2|G|^2$ and not dividing $\mathcal{B}_P$, then for any multiple $a \in \mathbb{Z}$ of $p_1 \cdots p_d$, there exists $b \in \mathbb{Z}$ such that $P(am+b, Y)$ is irreducible in $k[Y]$ for all integers m.*

This is to be related to question 1.1 (d) and effective HIT.

Theorem 5.2. *If y is suitably large (dep. on G), the number $N(G,y)$ of Galois extensions $E/\mathbb{Q}$ of group G and of discriminant $|d_E| \leq y$ obtained by specializing T to $t \in \mathbb{Z}$ in $F/k(T)$ satisfies*

$$N(G,y) \geq y^{\frac{1-(1/d)}{2d\deg_T(P)}}$$

Furthermore the counted extensions can be required to be totally split at every prime $p \in]p_0, \log y/(2d\deg_T(P))]$ (with p_0 dep. on G); and "to be totally split" can be more generally replaced by "to be of Frobenius in any prescribed conjugacy class of G".

This is to be related to question 1.1 (e) and the Malle conjecture.

5.3. **The self-twisted cover. Main reference:** [Dèb14]

References

[Dèb01] Pierre Dèbes. Théorème d'existence de Riemann. In *Arithmétique des revêtements algébriques*, volume 5 of *Séminaires et Congrès*, pages 27–41. SMF, 2001.

[Dèb09] Pierre Dèbes. Arithmétique des revêtements de la droite. 2009. at http://math.univ-lille1.fr/~pde/ens.html.

[Dèb14] Pierre Dèbes. On the Malle conjecture and the self-twisted cover. 2014.

[DG12] Pierre Dèbes and Nour Ghazi. Galois covers and the Hilbert-Grunwald property. *Ann. Inst. Fourier*, 62/3:989–1013, 2012.

[DL12] Pierre Dèbes and François Legrand. Twisted covers and specializations. In *Galois-Teichmueller theory and Arithmetic Geometry*, volume 63 of *Advanced Studies in Pure Math.*, pages 141–162. (H.Nakamura, F.Pop, L.Schneps, A.Tamagawa eds.), Mathematical Society of Japan, Tokyo, 2012.

[DL13] Pierre Dèbes and François Legrand. Specialization results in Galois theory. *Trans. A.M.S.*, 365/10:5259Ð5275, 2013.

[FJ04] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 2004. (second edition).

[GM71] Alexandre Grothendieck and Jacob P. Murre. *The Tame Fundamental Group of a Formal Neighbourhood of a Divisor with Normal Crossings on a Scheme*, volume 208 of *LNM*. Springer, 1971.

[Gro71] Alexandre Grothendieck. *Revêtements étales et groupe fondamental*, volume 224 of *LNM*. Springer, 1971.

[Lan83] Serge Lang. *Fundamentals of Diophantine Geometry*. Springer-Verlag, 1983.

[Sch00] Andrzej Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University, 2000.

E-mail address: `Pierre.Debes@math.univ-lille1.fr`

Laboratoire Paul Painlevé, Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France