PCMI 2022: AROUND THE INVERSE GALOIS PROBLEM

Diego Izquierdo

Instructions.

1. Read the course notes and try to do some of the exercises before coming to the exercise session. You may of course discuss the exercises with other participants.
2. During the session, form small groups of four or five to work together. It is important in mathematics to collaborate!
3. There are many exercises you can do in this booklet. You can of course choose those you want to work on in priority. To help you choose, I have indicated the difficulty of the exercises with stars. The exercises with 3 stars are bonus exercises that you should only do once you have done the others.
4. Sections 1 to 5 roughly correspond to the first class, sections 6 and 7 to the second, and sections 8 and 9 to the third.
5. Let me know if you find typos!

1 Warm-up: some explicit examples

Reminder 1.1 *Let K be a field and let G be a finite abstract group. We say that* ***the inverse Galois problem for*** *G* ***has a positive answer over*** *K if there exists a finite Galois extension L of K with Galois group G.*

Exercise 1: ⋆ *(Inverse Galois problem for abelian groups and cyclotomic extensions)*

1. Let ζ_n be a primitive n-th root of unity in $\mathbb{C}$. Recall what the Galois group of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is.
2. By using Dirichlet's Theorem on arithmetic progressions [1], prove that every finite abelian group is a quotient of $(\mathbb{Z}/n\mathbb{Z})^\times$ for some $n \geq 1$.
3. Solve the inverse Galois problem for finite abelian groups over $\mathbb{Q}$.

Exercise 2: ⋆ *(Symmetric group of prime order)*
Let p be a prime number.

1. For any two positive coprime integers a and d, there are infinitely many prime numbers of the form $a + nd$.

1. Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of degree p with exactly $p-2$ real roots. Prove that the Galois group of f over $\mathbb{Q}$ is isomorphic to $\mathscr{S}_p$.

2. Consider the polynomial $f = (X^2+m)\prod_{i=1}^{p-2}(X-n_i)$ for some positive integer m and some pairwise distinct integers $n_1, \dots, n_{p-2}$. For each prime number ℓ, introduce the polynomial $f_\ell = \ell^p f(X/\ell) + \ell$. Prove that, if ℓ is large enough, the Galois group of f_ℓ is isomorphic to $\mathscr{S}_p$.

2 Hilbert's irreducibility Theorem and Hilbertian fields

Reminder 2.1 *Let K be a field of characteristic* 0.

- *Let $f_1(T,X), \dots, f_r(T,X)$ be r irreducible polynomials in $K(T)[X]$. We introduce the subset $H_K(f_1, \dots, f_r)$ of K given by the elements $t \in K$ such that the polynomials $f_1(t,X), \dots, f_r(t,X)$ are all well-defined and irreducible in $K[X]$. The intersection of the set $H_K(f_1, \dots, f_r)$ with a Zariski open subset of K is called a* ***Hilbertian subset*** *of K.*
- *We say that K is* ***Hilbertian*** *if every Hilbertian subset of K is nonempty.* ***Hilbert's irreducibility Theorem*** *states that number fields are Hilbertian.*

Exercise 3: ⋆ *(Examples of non-Hilbertian fields)*

1. Prove that the maximal solvable extension $\mathbb{Q}_{\text{sol}}$ of $\mathbb{Q}$ is not Hilbertian.

2. Let K be a Henselian discretely valued field of characteristic 0.

(a) Let p be a prime number and let π be a uniformizer in K. Prove that, for each $a \in K^\times$, at least one of the two polynomials $f(X) = X^p + \pi a - 1$ and $g(X) = X^p + a^{-1} - 1$ has a root in K.

(b) Deduce that K is not Hilbertian.

Exercise 4: ⋆ *(Hilbertian fields and valuations)*
Let K be a Hilbertian field of characteristic 0 endowed with a valuation v. Prove that every Hilbertian subset of K is v-dense.
Hint: Let $H = H_K(f_1, \dots, f_m)$ be a Hilbertian subset of K, with $f_1, \dots, f_m$ irreducible polynomials in $K(T)[X]$. Given $a \in K$ and $\gamma = v(c) \in v(K^\times)$, consider the Hilbertian subset

$$H' := H_K(g_{i,\epsilon} : 1 \le i \le m, \epsilon \in \{\pm 1\})$$

of K, where $g_{i,\epsilon}(T,X) := f_i(a + cT^\epsilon, X)$.

Exercise 5: ⋆⋆ *(Finite extensions of Hilbertian fields)*
Let L/K be a finite extension of fields of characteristic 0. Let d be its degree and let S be a set of representatives of the quotient $\mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L)$. Take an irreducible polynomial $f \in L(T)[X]$.

1. (a) Assume that the $\sigma(f)$ for $\sigma \in S$ are pairwise relatively prime in $\overline{K(T)}[X]$. Prove that there exists an irreducible polynomial $p \in K(T)[X]$ such that $H_K(p) \subset H_L(f)$.

   (b) Prove that the same result still holds without the assumption that the $\sigma(f)$ for $\sigma \in S$ are pairwise relatively prime in $\overline{K(T)}[X]$.

   Hint: Prove that there exists $c \in L(T)$ such that the polynomials $\sigma(f(T, X + c))$ for $\sigma \in S$ are pairwise relatively prime in $\overline{K(T)}[X]$.

2. Prove that every Hilbertian subset of L contains a Hilbertian subset of K and deduce that, if K is Hilbertian, then so is L.

3. Let G be a finite group. Assume that K is Hilbertian and that there exists a finite Galois extension L of $K(T)$ in which K is algebraically closed and that has Galois group G. Prove that there are infinitely many pairwise linearly disjoint finite Galois extensions of K with Galois group G.

Exercise 6: ⋆⋆ *(Geometrical irreducibility and spreading out)*
Let K be a field.

1. Let $P_1, \dots, P_r$ be r polynomials in $K(T_1, \dots, T_n)[X_1, \dots, X_m]$, and assume that the system $\{P_i = 0, 1 \le i \le r\}$ (with variables $X_1, \dots, X_m$) has no solutions in the algebraic closure of $K(T_1, \dots, T_n)$. Prove that there is a non-empty Zariski open subset U of $\overline{K}^n$ such that the system

$$\{P_i(t_1, \dots, t_n, x_1, \dots, x_m) = 0, 1 \le i \le r\}$$

   is well-defined and has no solution in $\overline{K}$ for $(t_1, \dots, t_n) \in U$.

   Hint: Use the Nullstellensatz.

2. Let $f(T_1, \dots, T_n, X_1, \dots, X_m) \in K(T_1, \dots, T_n)[X_1, \dots, X_m]$ be an absolutely irreducible polynomial. Prove that there is a non-empty Zariski open subset U of $\overline{K}^n$ such that the polynomial $f(t_1, \dots, t_n, X_1, \dots, X_m)$ is well-defined and irreducible in $\overline{K}[X_1, \dots, X_m]$ for each $(t_1, \dots, t_n) \in U$.

3. Let $f(T_1, \dots, T_n, X_1, \dots, X_m) \in K(T_1, \dots, T_n)[X_1, \dots, X_m]$ be an irreducible polynomial. Is there necessarily a non-empty Zariski open subset U of K^n such that the polynomial $f(t_1, \dots, t_n, X_1, \dots, X_m)$ is well-defined and irreducible in $K[X_1, \dots, X_m]$ for each $(t_1, \dots, t_n) \in U$?

Exercise 7: ⋆⋆⋆ *(Function fields and Hilbertian subsets of K^n)*
Let K be a field of characteristic 0. In this exercise, we prove that the rational function field $K(U)$ is Hilbertian.

1. Let $f \in K[U, T, X]$ be a polynomial with $\deg_X f > 0$.

(a) Assume first that f is absolutely irreducible. By using the second question of exercise 6, prove that there exists a non-empty open subset U of $\overline{K}^2$ such that, for any pair $(a,b) \in U$, the polynomial $f(U, a+bU, X)$ is absolutely irreducible.

(b) Assume now that f is irreducible (but not necessarily absolutely irreducible). Prove that there exists a non-empty open subset U of K^2 such that, for any pair $(a,b) \in U$, the polynomial $f(U, a+bU, X)$ is irreducible over K.

2. Deduce from the previous question that the field $K(U)$ is Hilbertian.

3. Assume now that K is Hilbertian. Let $f_1(T_1,\dots,T_n,X),\dots,f_r(T_1,\dots,T_n,X)$ be r irreducible polynomials in $K(T_1,\dots,T_n)[X]$. Use the previous question to prove that the subset $H_K(f_1,\dots,f_r)$ of K^n given by the elements $(t_1,\dots,t_n) \in K^n$ such that the polynomials

$$f_1(t_1,\dots,t_n,X),\dots,f_r(t_1,\dots,t_n,X)$$

are all well-defined and irreducible in $K[X]$ is Zariski dense in K^n.

Remark: this last question shows that Theorem 1.4 of the course notes implies Corollary 1.5.

3 Noether's problem

Reminder 3.1

- *Let L/K be a field extension. We say that L is **rational** (or **pure**) over K if L is K-isomorphic to the field of rational functions $K(x_1,\dots,x_n)$ for some n. We say that L is **stably rational** if there exists an integer m such that the field of rational functions $L(y_1,\dots,y_m)$ is rational over K.*
- *Let K be a field and let G be a finite abstract group of order n. We make G act on the field $K(x_1,\dots,x_n)$ by permuting the coordinates. We say that **Noether's problem has a positive answer for** G **over** K if the fixed field $K(x_1,\dots,x_n)^G$ is rational (or stably rational) over K. In that case, the inverse Galois problem for G also has a positive answer over K.*
- *The **no-name lemma** states that, if the fixed field $K(V)^G$ is stably rational for **some** faithful representation V of G, then the same result holds for **any** faithful representation of G. Noether's problem is the particular case of the regular representation.*

Exercise 8: ⋆ *(Noether's problem for symmetric groups)*
Prove that Noether's problem has a positive answer for symmetric groups over number fields.

Exercise 9: ⋆ *(Noether's problem for $\mathbb{Z}/3\mathbb{Z}$ over $\mathbb{C}$)*
The goal of this exercise is to prove that Noether's problem holds for the group $\mathbb{Z}/3\mathbb{Z}$ over $\mathbb{C}$. To do so, make $A = \mathbb{Z}/3\mathbb{Z}$ act on $\mathbb{C}(x_1, x_2, x_3)$ cyclically. Let j be a primitive third root of unity and introduce the elements:

$$\begin{cases} e_1 = x_1 + x_2 + x_3 \\ e_2 = x_1 + jx_2 + j^2 x_3 \\ e_3 = x_1 + j^2 x_2 + jx_3. \end{cases}$$

1. Prove that $\mathbb{C}[x_1, x_2, x_3] = \mathbb{C}[e_1, e_2, e_3]$.
2. Compute the action of A on an element of $\mathbb{C}[x_1, x_2, x_3]$ of the form $e_1^n e_2^m e_3^p$.
3. Deduce that $\mathbb{C}[x_1, x_2, x_3]^A = \mathbb{C}[e_1, e_2 e_3, e_2^3]$.
4. Deduce that $\mathbb{C}(x_1, x_2, x_3)^A = \mathbb{C}(e_1, e_2 e_3, e_2^3)$.

Exercise 10: ⋆ *(Fischer's Theorem over the complex numbers)*
The goal of this exercise is to prove that Noether's problem holds for all finite abelian groups over $\mathbb{C}$ by generalizing the argument of the previous exercise. To do so, fix a finite abelian group A, consider an embedding $A \subset \mathscr{S}_n$ for some integer n and make A act on $V := \mathbb{C}^n$ by permuting the coordinates.

1. Explain why there is a basis $(e_1, \dots, e_n)$ of V and characters $\chi_1, \dots, \chi_n \in \mathrm{Hom}(A, \mathbb{C}^\times)$ such that:
$$\forall a \in A, \forall \lambda_1, \dots, \lambda_n \in \mathbb{C}, a \cdot \left(\sum_i \lambda_i e_i \right) = \sum_i \chi_i(a) \lambda_i e_i.$$
2. Let G be the subgroup of $\mathbb{C}(V)^\times$ spanned by $e_1, \dots, e_n$. Check that G is a free abelian group of rank n.
3. Let H be the kernel of the morphism $\varphi : G \to \mathrm{Hom}(A, \mathbb{C}^\times)$ that sends each e_i to χ_i. Prove that $\mathbb{C}(V)^A = \mathbb{C}(H)$.
4. Deduce that Noether's problem has a positive answer for A over $\mathbb{C}$.
5. Given a number field K, do the previous arguments still hold when one replaces $\mathbb{C}$ by K?

Exercise 11: ⋆ *(Noether's problem for Q_8)*
Let K be a field of characteristic other than 2. Let $\mathbb{H}$ be Hamilton's quaternion algebra over K and let $\mathbf{H}^\times$ be the multiplicative group of $\mathbb{H}$, seen as an algebraic group over K. Denote by Q_8 the quaternion group and set $X := \mathbf{H}^\times / Q_8$.

1. Prove that $X \cong \mathbb{G}_\mathrm{m} \times \mathrm{SO}_3 / G$ where G is the finite group:
$$G = \left\{ 1, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

Hint: consider the morphism $(N,\phi) : \mathbf{H}^\times \to \mathbb{G}_m \times \mathrm{SO}_3$ *in which* N *is the reduced norm and* ϕ *maps a quaternion* x *to the rotation* $y \mapsto xyx^{-1}$ *on the 3-dimensional vector space of quaternions of trace 0.*

2. Prove that X is a rational variety and deduce that Noether's problem has a positive answer for Q_8 over K.

Exercise 12: ⋆ *(Noether's problem for dihedral groups)*
Let K be a field and G a finite group.

1. Consider an action of G on the polynomial ring $K[t]$ such that K is stable under the action of G. Prove that there exists a G-invariant polynomial f such that $K(t)^G = K^G(f)$.

2. Consider a linear action of G on a finite dimensional K-vector space V. Prove that $K(V)^G$ is a purely transcendental extension of $K(\mathbb{P}(V))^G$.

3. Deduce that Noether's problem has a positive answer for every finite subgroup of $\mathrm{GL}_2(K)$. In particular, this applies to the dihedral groups D_{2n} when K is algebraically closed or when $K = \mathbb{R}$.

Exercise 13: ⋆⋆ *(Noether's problem for* $\mathscr{A}_5$*)*

1. By proceeding as in the previous exercise, prove that Noether's problem has a positive answer for every finite subgroup of $\mathrm{GL}_3(\mathbb{C})$ over $\mathbb{C}$. You may use without proof Castelnuovo's Theorem [2].

2. Deduce that Noether's problem has a positive answer for the alternating group $\mathscr{A}_5$ over $\mathbb{C}$. This result is due to Maeda.

Exercise 14: ⋆⋆⋆ *(No-name lemma)*
This exercise aims at proving the no-name lemma. Let K be a field.

1. Let L/K be a finite Galois extension with Galois group G. Prove that, for any finite dimensional L-vector space V and any semi-linear action [3] of G on V, there is a canonical isomorphism:

$$V \cong V^G \otimes_K L.$$

Deduce that the extension $L(V)^G/K = K(V^G)/K$ is purely transcendental. This statement is called *Speiser's Lemma.*

2. Let G be a finite group. Let V and W be two faithful finite-dimensional linear representations of G over K. Deduce from question 1 that the fields $K(V)^G$ and $K(W)^G$ are stably equivalent [4].

2. Over an algebraically closed field, a unirational surface, that is a surface that is dominated by a rational variety, is rational.

3. An action of G on V such that $\sigma \cdot (\lambda v) = \sigma(\lambda)(\sigma \cdot v)$ for $\sigma \in G$, $\lambda \in L$ and $v \in V$.

4. This means that there exist integers n and m such that $K(V)^G(x_1,\dots,x_n) \cong K(W)^G(y_1,\dots,y_m)$.

Remark 1: Geometrically, this means that, if we consider two embeddings $G \hookrightarrow \mathrm{GL}_p(K)$ and $G \hookrightarrow \mathrm{GL}_q(K)$ and we set $X_1 := \mathbb{A}_K^p/G$ and $X_2 := \mathbb{A}_K^q/G$, then there exist integers m and n such that $X_1 \times \mathbb{A}_K^m$ and $X_2 \times \mathbb{A}_K^n$ are birationally equivalent. We say that X_1 and X_2 are ***stably birational****.*

Remark 2: The no-name lemma can also be used to study a quotient of the form $X_3 := \mathrm{SL}_r/G$ for some embedding $G \hookrightarrow \mathrm{SL}_r(K)$. If you wish, you can try to prove by yourself that X_1 and X_3 are stably birational.

4 Versal torsors

Reminder 4.1 *Let G be a finite abstract group, K an infinite field, and X a K-variety. A G-torsor $f : Y \to X$ is called* ***versal*** *if, for every extension L/K and for every G-torsor $P \to \operatorname{Spec} L$, there exists an L-point Q in X such that the fiber $X_Q := f^{-1}(Q)$ is isomorphic to the G-torsor $P \to \operatorname{Spec} L$.*

Exercise 15: ⋆ *(A torsor under $\mathbb{Z}/2\mathbb{Z}$)*
Let K be an infinite field. Make $G := \mathbb{Z}/2\mathbb{Z}$ act on $X := \mathbb{A}_K^1 \setminus \{-1,0,1\}$ by $\sigma \cdot x = x^{-1}$, where σ is a generator of G. Consider the G-torsor $X \to X/G$. Depending on the characteristic of K, decide whether it is versal.

Exercise 16: ⋆⋆ *(Versal torsors and twisting)*
Let K be an infinite field and G a finite abstract group.

1. Consider X a quasi-projective K-variety endowed with an action of G, and P a G-torsor over K. We define the **twist** ${}_PX$ of X by P as the quotient $(X \times P)/G$. The natural map $X \times P \to {}_P X$ makes $X \times P$ into a G-torsor over ${}_PX$. Prove that there is a bijection between the set of K-rational points ${}_PX(K)$ and the set of G-equivariant morphisms $P \to X$.

   Hint: when you start with a point $Q \in {}_P X(K)$, you may consider its fiber Y_Q in $Y := X \times P$, construct a G-equivariant morphism from Y_Q to P, and use the general fact that every G-equivariant morphism between two G-torsors over K is an isomorphism.
2. Let now X be a K-variety and $f : Y \to X$ a G-torsor. Deduce from the previous question that f is versal if, and only if, for every field extension L/K and every G-torsor P over L, the set of L-rational points ${}_PX(L)$ is non-empty.

Exercise 17: ⋆⋆ *(A torsor under $\mathbb{Z}/3\mathbb{Z}$)*
Let K be an infinite field. Consider the action of $G := \mathbb{Z}/3\mathbb{Z}$ on $\mathbb{P}_K^1$ defined by:

$$\sigma \cdot [x : y] = [y : y - x],$$

where σ is a generator of G. Let U be a G-stable open subset of $\mathbb{P}_K^1$ on which the action is free and consider the G-torsor $\pi : U \to V := U/G$. Let P be a G-torsor over K.

1. Prove that the twist ${}_P\mathbb{P}^1_K$ is a genus 0 smooth projective curve that has a point in a degree 3 extension of K.

   Hint: you may observe that, in general, when you twist a variety X endowed with an action of G by the trivial G-torsor, you get a variety that is isomorphic to X.

2. By using the Riemann-Roch Theorem, deduce that ${}_P\mathbb{P}^1_K$ is a projective line.

3. Deduce that the set of rational points $Q \in V(K)$ such that the the fiber U_Q is isomorphic to P as a G-torsor is non-empty. This shows that $\pi : U \to V$ is a versal G-torsor.

Exercise 18: ⋆⋆ *(Versal torsors and Noether's problem)*
Let K be an infinite field and let G be a finite group. Consider a generically free linear action of G on $\mathbb{A}^n_K$. Let U be an open subset of $\mathbb{A}^n_K$ on which G acts freely, consider the G-torsor $\pi : U \to V := U/G$, and take a G-torsor P over K.

1. Prove that the twist ${}_P\mathbb{A}^n_K$ is isomorphic to $\mathbb{A}^n_K$.

   Hint: recall that, by Hilbert's Theorem 90, every GL_n*-torsor over a field is trivial.*

2. Deduce that the set of rational points $Q \in V(K)$ such that the the fiber U_Q is isomorphic to P as a G-torsor is non-empty. This shows that $U \to V$ is a versal G-torsor.

5 Grunwald-Wang problem

Reminder 5.1 *Let K be a number field and let G be a finite abstract group. We say that **the Grunwald-Wang problem for G has a positive answer over K** if, whenever we are given a finite set S of places of K and a Galois extension L_v/K_v for each $v \in S$ whose Galois group can be embedded into G, one can find a Galois field extension L/K with Galois group G such that the completion of L/K at any place of L lying above a place $v \in S$ is isomorphic to L_v/K_v. A positive answer to Noether's problem implies a positive answer to the Grunwald-Wang problem, which itself implies a positive answer to the inverse Galois problem.*

Exercise 19: ⋆ *(An explicit example)*
Find an explicit Galois extension K of $\mathbb{Q}$ with Galois group $\mathscr{S}_3$ such that, if v_p stands for a place of K above p for each prime number p, then:

$$K_{v_3} \cong \mathbb{Q}_3(\sqrt{2}), \quad K_{v_5} \cong \mathbb{Q}_5(\sqrt[3]{5}, j), \quad K_{v_7} \cong \mathbb{Q}_7(\zeta_9), \quad K_{v_{11}} \cong \mathbb{Q}_{11},$$

where j is a primitive third root of unity and ζ_9 is a primitive 9-th root of unity.

Exercise 20: ⋆⋆ *(Wang's counter-example)*
Let $L/\mathbb{Q}$ be a Galois extension with Galois group $G = \mathbb{Z}/8\mathbb{Z}$. Assume by contradiction that the prime 2 is unramified.

1. Prove that L contains the field $K := \mathbb{Q}(\sqrt{m})$ for some integer m such that $m \equiv 5 \mod 8$.
2. Let p be a prime divisor of m.
   (a) Prove that p is totally ramified in L.
   (b) Let $\mathfrak{p}$ be the unique prime ideal of L lying above p and let $L_{\mathfrak{p}}$ be the completion of L at $\mathfrak{p}$. Let U be the unit group of $\mathscr{O}_{L_{\mathfrak{p}}}$. Prove that the order of $H^1(G,U)$ is divisible by 8.
   (c) Prove that there exists an injective morphism $H^1(G,U) \to H^1(G,\mathbb{F}_p^\times)$.
   (d) Deduce that 8 divides $p-1$.
3. Get a contradiction!
4. Does Noether's problem for $\mathbb{Z}/8\mathbb{Z}$ over $\mathbb{Q}$ have a positive answer?

6 Regular inverse Galois problem

Reminder 6.1 *Let K be a field and let G be a finite abstract group. We say that a finite Galois extension L of K(t) is* ***regular*** *if K is algebraically closed in L. We say that* ***the regular inverse Galois problem for*** *G* ***has a positive answer over*** *K if there exists a finite regular Galois extension L of K(t) with Galois group G. A positive answer to Noether's problem implies a positive answer to the regular inverse Galois problem, which itself implies a positive answer to the inverse Galois problem.*

Exercise 21: ⋆ *(Regular inverse Galois problem for products)*
Let K be a field. Let G_1 and G_2 be two finite groups for which the regular Galois problem over K has a positive answer. Prove that the regular Galois problem for $G_1 \times G_2$ over K also has a positive answer.
Hint: study the ramification of some given solutions to the regular Galois problems for the groups G_1 and G_2.

Exercise 22: ⋆ *(The regular inverse Galois problem for $\mathscr{A}_n$)*
Let K be a number field. Consider the polynomial $f(X,T) = (n-1)X^n - nX^{n-1} + T$ and let G be the Galois group of $f(X,t)$ over $K(t)$. In order to compute G, we introduce the curve C given by the equation $f(x,t) = 0$ and the finite cover $\pi : C \to \mathbb{A}^1$ that sends (x,t) to t.

1. Prove that π is étale outside 0 and 1.

2. By studying the ramification of π at 0 and 1, prove that $G = \mathscr{S}_n$.

3. Prove that the field fixed by the subgroup $\mathscr{A}_n$ of G is rational, and deduce that the regular inverse Galois problem for $\mathscr{A}_n$ over K has a positive answer. This result was first proved by Hilbert.

Hint: compute the discriminant of $f(X,T) \in K(T)[X]$.

4. More generally, use the Riemann-Hurwitz formula [5] to prove the *double group trick*: if G is the Galois group of a regular extension L of $K(T)$ ramified at most at three places which are rational over K, and if H is a subgroup of G of index 2, then the fixed field L_1 of H is rational, and hence the regular inverse Galois problem for H has a positive answer.

Exercise 23: ⋆⋆ *(Regular inverse Galois problem for abelian groups)*
Let K be a number field. In this exercise, we prove that the regular inverse Galois problem has a positive answer for finite abelian groups over K.

1. Let B be a finite Galois module [6] over K. This question aims at proving that there exists an exact sequence of Galois modules:

$$0 \to P \to F \to B \to 0$$

in which P and F are finitely generated and torsion-free as abelian groups and P is a permutation module [7].

(a) Prove that there exists an exact sequence:

$$0 \to D \to C \to B \to 0$$

in which C and D are finitely generated torsion-free Galois modules.

(b) Prove that there exists an exact sequence:

$$0 \to D \to P \to E \to 0$$

in which E and P are finitely generated torsion-free Galois modules and P is a permutation module.

5. Let K be a field of characteristic 0. Let C_1 and C_2 be two smooth projective K-curves with respective genera g_1 and g_2, and consider a non-constant morphism $\phi : C_1 \to C_2$. Then:

$$2g_1 - 2 = \deg(\phi) \cdot (2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1)$$

where $e_\phi(P)$ is the ramification index of ϕ at P.

6. An abelian group on which $\mathrm{Gal}(\overline{K}/K)$ acts compatibly and continuously.

7. A Galois module that has a Galois-stable $\mathbb{Z}$-basis.

(c) Let F be the amalgamated sum of C and P over D. Check that F is torsion-free and prove that there is an exact sequence:

$$0 \to P \to F \to B \to 0.$$

2. Let A be a finite abelian group. By using question 1, prove that there exists an exact sequence:

$$1 \to A \to T \to Q \to 1$$

in which T and Q are K-tori and Q is quasi-trivial [8].

Hint: Recall that one defines an equivalence of categories between groups of multiplicative type and finitely generated Galois modules by sending a group of multiplicative type to its character module.

3. Deduce from question 2 that the regular inverse Galois problem for A over K has a positive answer.

Exercise 24: ⋆⋆⋆ *(Regular inverse Galois problem for groups of order p^3)*
Let K be a number field and consider a split exact sequence of finite groups:

$$1 \to A \to H \to G \to 1,$$

so that H is the semi-direct product $A \rtimes G$ for some action of G on A. Assume that A is abelian and that the regular inverse Galois problem for G has a positive answer. This means that there exists an open subset U of $\mathbb{P}^1_K$ and a regular étale G-covering $\pi : C \to U$.

1. In this question, we assume that $A = \prod_{g \in G} B$ and that G acts on A by permuting the coordinates. Question 2 of the previous exercise then gives an exact sequence:

$$1 \to B \to T \to Q \to 1$$

in which T and Q are tori and Q is quasi-trivial. Construct a free action of H on $X := \left(\prod_{g \in G} T\right) \times C$ such that $Y := X/H$ is rational. Deduce that the regular inverse Galois problem for H has a positive answer.

2. We do not assume anymore that $A = B^G$. Prove that the regular inverse Galois problem for H still has a positive answer.

3. Let now H' be a finite group that is generated by a normal abelian subgroup A' and by a subgroup G' for which the regular inverse Galois problem has a positive answer. Prove that the regular inverse Galois problem for H' also has a positive answer.

8. A torus whose character module is a permutation module.

4. Let p be a prime number. Deduce from the previous question that the regular inverse Galois problem has a positive answer for all groups of order p^3. This result is due to Schneps.

Exercise 25: ⋆ ⋆ ⋆ *(From PAC fields of characteristic 0 to finite fields)*
A characteristic 0 field K is said to be *pseudo-algebraically closed* (PAC) if each geometrically irreducible variety V defined over K has a rational point. In 1991, Fried and Völklein proved that the regular inverse Galois problem has a positive answer over characteristic 0 PAC fields. In this exercise, we aim at deducing that every finite group G is a regular Galois group over $\mathbb{F}_p(t)$ for almost all p.

1. (a) Let L be a field. Construct a field $\phi(L)$ such that every geometrically irreducible L-variety has a $\phi(L)$-point and L is algebraically closed in $\phi(L)$.

(b) Construct a PAC field K of characteristic 0 in which $\mathbb{Q}$ is algebraically closed.

2. Let G be a finite group.

(a) Use the previous question and Fried and Völklein's Theorem on PAC fields to prove that there exists a finitely generated $\mathbb{Z}$-algebra B, an irreducible scheme $\mathscr{C}$ and a finite morphism $f : \mathscr{C} \to \mathbb{P}^1_B$ satisfying the following properties:

i. the fibers of $\mathscr{C} \to \operatorname{Spec} B$ are geometrically irreducible,

ii. for each closed point $b \in \operatorname{Spec} B$, the function field of the fiber $\mathscr{C}_b$ is a Galois extension with Galois group G of the function field of the fiber $(\mathbb{P}^1_B)_b$,

iii. almost every fiber of $\operatorname{Spec} B \to \operatorname{Spec} \mathbb{Z}$ is geometrically irreducible.

Hint: Use exercise 6.

(b) Prove that $\operatorname{Spec} B$ has an $\mathbb{F}_p$-point for almost every prime number p.

Hint: Use the Lang-Weil estimates.

(c) Deduce from (a) and (b) that G is a regular Galois group over $\mathbb{F}_p(t)$ for almost every prime number p.

7 Rigidity method

Reminder 7.1 *Let G be a finite group* ***with trivial center****. Denote its order by n.*

- *Let* $\mathscr{C}$ *be the set of conjugation classes of G. We consider the action of the group* $\Gamma := \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ *on G which sends each* $g \in G$ *to* g^r *for* $r \in \Gamma$*. It also induces an action on* $\mathscr{C}$*. A conjugation class of G is said to be* ***rational*** *if it is fixed by this action.*

- *Let $(C_1,\dots,C_r)$ be a finite sequence of conjugacy classes of G. Let Σ be the set of r-tuples $(g_1,\dots,g_r)\in C_1\times\cdots\times C_r$ such that $G=\langle g_1,\dots,g_r\rangle$ and $g_1\dots g_r=1$. We say that $(C_1,\dots,C_r)$ is* ***rigid*** *if $\Sigma\neq\emptyset$ and the action of G on Σ by conjugation is transitive.*
- ***Rigidity Theorem (Belyi, Fried, Matzat, Shih, Thompson).*** *Let K be a field of characteristic 0. Let $(C_1,\dots,C_r)$ be a rigid family of rational conjugacy classes of G, and let $P_1,\dots,P_r$ be distinct rational points in $\mathbb{P}^1_K$. Then there exists a regular Galois extension L of $K(t)$ with Galois group G that is unramified outside $P_1,\dots,P_r$ and such that the inertia subgroup at P_i is generated by an element of C_i for each i.*
- *More generally, let $(C_1,\dots,C_r)$ be a rigid family of conjugacy classes of G and let $P_1,\dots,P_r$ be r distinct points in $\mathbb{P}^1_K$. Assume that the set $\{C_1,\dots,C_r\}$ is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, that the set $\{P_1,\dots,P_r\}$ is stable under the action of $\mathrm{Gal}(\overline{K}/K)$, and that the $\mathrm{Gal}(\overline{K}/K)$-sets $\{C_1,\dots,C_r\}$ and $\{P_1,\dots,P_r\}$ are isomorphic. Then there exists a regular Galois extension L of $K(t)$ with Galois group G that is unramified outside $P_1,\dots,P_r$ and such that the inertia subgroup at P_i is generated by an element of C_i for each i.*

Exercise 26: $\star$ *(Rigidity)*
We keep the notations of the previous reminder. Prove that G acts freely on Σ. Deduce that $(C_1,\dots,C_r)$ is rigid if, and only if, $|\Sigma|=|G|$.

Exercise 27: $\star$ *(On the assumption about the triviality of the center)*
Prove that every finite group is a quotient of a finite group with trivial center.
Hint: consider well-chosen wreath products.
Remark: this exercise shows that the assumption about the triviality of the center in the rigidity method is not a big deal.

Exercise 28: $\star$ *(Rigidity for the symmetric group)*
Let $n\geq 4$ be an integer.

1. Prove that every conjugacy class in $\mathscr{S}_n$ is rational.
2. Let C_2, C_{n-1} and C_n be the conjugation classes of transpositions, $(n-1)$-cycles and n-cycles respectively. Prove that the triple (C_n,C_2,C_{n-1}) is rigid.
3. Thanks to the rigidity method, deduce that, for every characteristic 0 field K, the group $\mathscr{S}_n$ is the Galois group of a regular extension of $K(t)$. What local conditions can one impose?

Exercise 29: $\star\star$ *(Rigidity for $\mathscr{A}_5$)*
In the alternating group $\mathscr{A}_5$, let C_2 be the conjugation class of double transpositions and C_5 and C'_5 the two conjugation classes of 5-cycles.

1. Prove that the set $\{C_2, C_5, C_5'\}$ is stable under the action of the absolute Galois group of $\mathbb{Q}$.
2. Prove that the triple (C_2, C_5, C_5') is rigid.
3. Thanks to the rigidity method, deduce that the group $\mathscr{A}_5$ is the Galois group of a regular extension of $\mathbb{Q}(t)$. What local conditions can one impose?

8 Weak approximation

Reminder 8.1 *Let K be a number field.*

- *Let X be a smooth variety over K. We say that X satisfies **weak approximation** if, for every non-empty finite set S of places of K, the set of rational points $X(K)$ is dense in the product $\prod_{v\in S} X(K_v)$ (where each $X(K_v)$ is endowed with the v-adic topology).*
- *Let G be a finite group. Embed it in SL_n for some n. Then the Grunwald-Wang problem for G over K has a positive answer if, and only if, the homogeneous space $X := \mathrm{SL}_n/G$ satisfies weak approximation.*

Exercise 30: ⋆ *(Artin-Whaples approximation Theorem)*
Let K be a number field.

1. Let $|\cdot|_1, \dots, |\cdot|_n$ be n inequivalent nontrivial absolute values of K. Prove that there exists $a \in K$ such that $|a|_1 > 1$ and $|a|_i < 1$ for $i > 1$.
2. Prove that the affine line $\mathbb{A}^1_K$ satisfies weak approximation.

Exercise 31: ⋆ *(Weak approximation, birationality, and retract rationality)*

1. Let X and Y be two smooth varieties over a number field K. Assume that X and Y are stably birational, that is there exist integers m and n such that $X \times \mathbb{A}^m_K$ and $Y \times \mathbb{A}^n_K$ are birationally equivalent. Prove that X has weak approximation if, and only if, so does Y.
2. Prove that smooth retract rational varieties defined over number fields satisfy weak approximation.

Exercise 32: ⋆⋆ *(Cohomological interpretation of weak approximation)*
Let K be a number field.

1. Let F be a finite algebraic group over K and embed it in SL_n. Consider the homogeneous space $X := \mathrm{SL}_n/F$. Prove that X satisfies weak approximation if, and only if, the restriction map:

$$H^1(K, F) \to \prod_{v\in S} H^1(K_v, F)$$

is surjective for every non-empty finite set of places S of K. In that case, we say that F **satisfies weak approximation**.

Hint: Consider the sequence $1 \to F \to \mathrm{SL}_n \to X \to 1$ *and write the non-abelian cohomology exact sequence associated to it.*

2. Deduce that, for each integer $n \geq 1$, the group μ_n satisfies weak approximation.

3. Can you find an integer n such that $\mathbb{Z}/n\mathbb{Z}$ does not satisfy weak approximation over $\mathbb{Q}$?

Exercise 33: ⋆⋆⋆ *(Weak weak approximation)*
Let K be a number field. One says that a smooth K-variety X satisfies the *weak weak approximation property* if there exists a finite set of places S_0 of K such that, for every finite set of places S of K that does not intersect S_0, the set $X(K)$ is dense in $\prod_{v\in S} X(K_v)$.

1. Let F be a finite algebraic group over K. Embed it in SL_n and consider the homogeneous space $X := \mathrm{SL}_n/F$. By proceeding as in the previous exercise, prove that X has the weak weak approximation property if, and only if, there exists a finite set of places S_0 of K such that, for every non-empty finite set of places S of K that does not intersect S_0, the diagonal map:

$$H^1(K,F) \to \prod_{v\in S} H^1(K_v,F)$$

is surjective. In that case, we say that F **satisfies weak weak approximation**.

In the following questions, we aim at proving that, if F is abelian, then it satisfies the weak weak approximation property. This result is due to Neukirch.

2. Let S be a finite set of places of K, set $F' := \mathrm{Hom}(F, \overline{K}^{\times})$, and introduce the Tate-Shafarevich groups:

$$Ш^1(K,F') := \ker\left(H^1(K,F') \to \prod_{v} H^1(K_v,F')\right),$$
$$Ш^1_S(K,F') := \ker\left(H^1(K,F') \to \prod_{v\notin S} H^1(K_v,F')\right).$$

By using Tate's local duality Theorem [9] and the Poitou-Tate exact sequence [10], prove that, for each non-empty finite set of places S of K, the diagonal map:

$$H^1(K,F) \to \prod_{v\in S} H^1(K_v,F)$$

9. Let K be a local field of characteristic 0 and M a finite Galois module over K. Set $M' := \mathrm{Hom}(M, \overline{K}^{\times})$. Then the cup-product induces a perfect pairing of finite groups:

$$H^1(K_v,M) \times H^1(K_v,M') \to \mathrm{Br}\, K_v \subset \mathbb{Q}/\mathbb{Z}.$$

10. Let K be a number field and M a finite Galois module over K. Set $M' := \mathrm{Hom}(M, \overline{K}^{\times})$. Then there

is surjective if, and only if, $Ш^1(K,F') = Ш^1_S(K,F')$.

3. Let L be a finite Galois extension of K over which F' splits [11]. For each finite set of places S of K, prove that:

$$Ш^1(K,F') = Ш^1(L/K,F') \quad \text{and} \quad Ш^1_S(K,F') = Ш^1_S(L/K,F')$$

where:

$$Ш^1(L/K,F') := \ker\left(H^1(L/K,F') \to \prod_{w|v} H^1(L_w/K_v,F')\right),$$
$$Ш^1_S(L/K,F') := \ker\left(H^1(L/K,F') \to \prod_{w|v, v\notin S} H^1(L_w/K_v,F')\right).$$

4. Assume now that S does not contain those places that ramify in L. Prove that:

$$Ш^1_S(L/K,F') = Ш^1(L/K,F').$$

5. Conclude that F satisfies the weak weak approximation property.

Exercise 34: ⋆ ⋆ ⋆ *(Hyper-weak approximation)*
Let K be a number field and let F be a finite group, that we see as a finite constant K-group. Following Harari, we say that F has the *hyper-weak approximation property* if there exists a finite set of places S_0 of K such that, for every non-empty finite set of places S of K that does not intersect S_0, the image of the diagonal map:

$$H^1(K,F) \to \prod_{v\in S} H^1(K_v,F)$$

contains $\prod_{v\in S} H^1(K_v^{\mathrm{nr}}/K_v,F)$.

---

is an exact sequence:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(K,M) & \longrightarrow & \prod_v H^0(K_v,M) & \longrightarrow & H^2(K,M')^D \\ & & & & & & \downarrow \\ & & H^1(K,M')^D & \longrightarrow & \prod'_v H^1(K_v,M) & \longrightarrow & H^1(K,M) \\ & & \downarrow & & & & \\ & & H^2(K,M) & \longrightarrow & \bigoplus_v H^2(K_v,M) & \longrightarrow & H^0(K,M')^D \longrightarrow 0, \end{array}$$

where the restricted product is computed with respect to the $H^1(\mathcal{O}_v,M)$ and $-^D := \mathrm{Hom}(-,\mathbb{Q}/\mathbb{Z})$ is the Pontryagyn duality.

11. This means that $\mathrm{Gal}(\overline{K}/L)$ acts trivially on F'.

1. Prove that, if F satisfies the hyper-weak approximation property, then it is the Galois group of some finite Galois extension L of K.

   Hint: you may use the following classical result about abstract finite groups: if H is a subgroup of a finite group G and if H intersects all the conjugation classes of G, then $H = G$.

2. Prove that quotients of a group satisfying the hyper-weak approximation property also satisfy the hyper-weak approximation property.

3. Consider a split exact sequence of finite groups:

$$1 \to A \to E \to G \to 1$$

   in which A is abelian and G satisfies the hyper-weak approximation property. Prove that E satisfies the hyper-weak approximation property.

   Hint: use exercise 33.

9 The Brauer-Manin obstruction

Reminder 9.1 *Let K be a number field, X a smooth K-variety and G a finite abstract group.*

- *Let X_c be a smooth compactification of X. The **unramified Brauer group** of X is defined as the étale cohomology group $\mathrm{Br}_{\mathrm{nr}} X := H^2(X_c, \mathbb{G}_m)$. It can also be computed thanks to the exact sequence:*

$$0 \to \mathrm{Br}_{\mathrm{nr}} X \to \mathrm{Br}\, K(X) \to \bigoplus_{v \in X_c^{(1)}} H^1(K(v), \mathbb{Q}/\mathbb{Z})$$

  where $X_c^{(1)}$ is the set of codimension 1 points in X_c and the second arrow is induced by the residue maps. It is a stable birational invariant, and hence we also denote $\mathrm{Br}_{\mathrm{nr}} K(X)$ instead of $\mathrm{Br}_{\mathrm{nr}} X$.

- *Consider an embedding of G in some SL_n. Set $X := \mathrm{SL}_n/G$. The following two theorems are helpful to compute the unramified Brauer group of X.*

  ***Theorem (Bogomolov).** Let $\mathscr{B}_G$ be the set of bicyclic subgroups of G (i.e. those subgroups of G that are spanned by at most two elements). Then:*

$$\mathrm{Br}_{\mathrm{nr}} \overline{X} \cong \ker\left(H^3(G, \mathbb{Z}) \to \prod_{H \in \mathscr{B}_G} H^3(H, \mathbb{Z}) \right).$$

  ***Theorem (Harari).** Let G^{ab} be the abelianization of G and set $M := \mathrm{Hom}(G^{\mathrm{ab}}, \overline{K}^\times)$. Consider the algebraic unramified Brauer group of X:*

$$\mathrm{Br}_{\mathrm{nr}_1} X := \ker\left(\mathrm{Br}_{\mathrm{nr}} X \to \mathrm{Br}_{\mathrm{nr}} \overline{X} \right).$$

Then the quotient $\mathrm{Br}_{\mathrm{nr}_1} X/\mathrm{Br}\,K$ *is isomorphic to the subgroup of* $H^1(K,M)$ *given by those elements a whose restriction* $a_v \in H^1(K_v,M)$ *is orthogonal*[12] *to the image* $\mathrm{im}\left(H^1(K_v,G)\to H^1(K_v,G^{\mathrm{ab}})\right)$ *for almost all* v.

- *The* ***Brauer-Manin pairing*** *is defined by:*

$$\begin{aligned}\mathrm{BM} : X(K_\Omega)\times \mathrm{Br}_{\mathrm{nr}} X &\to \mathbb{Q}/\mathbb{Z}\\ ((p_v)_v,\alpha) &\mapsto \sum_v j_v(p_v^*\alpha),\end{aligned}$$

where $X(K_\Omega) := \prod_v X(K_v)$ *and* $j_v : \mathrm{Br}\,K_v \to \mathbb{Q}/\mathbb{Z}$ *is the local invariant. The Brauer-Manin pairing is continuous with respect to the* v*-adic topologies on the* $X(K_v)$. *The* ***Brauer-Manin set*** $X(K_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$ *of* X *is the orthogonal of* $\mathrm{Br}_{\mathrm{nr}} X$ *with respect to* BM. *It always contains the set of rational points of* X.

- *We say that G is* ***supersolvable*** *if there exists a normal series*

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_{r-1} \lhd H_r = G$$

such that each quotient group H_{i+1}/H_i *is cyclic and each* H_i *is normal in* G.

- ***Theorem (Harpaz-Wittenberg).*** *Assume that G is supersolvable and consider an embedding of G in some* SL_n. *Set* $X := \mathrm{SL}_n/G$. *Then* $X(K)$ *is dense in* $X(K_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$.

Exercise 35: ⋆ *(Brauer-Manin obstruction and weak weak approximation)*
Let K be a number field and let X be a smooth K-variety such that $X(K)$ is a dense non-empty subset of $X(K_\Omega)^{\mathrm{Br}_{\mathrm{nr}}}$. Assume that $\mathrm{Br}_{\mathrm{nr}} X/\mathrm{Br}\,K$ is finite. Prove that X satisfies the weak weak approximation property.

Exercise 36: ⋆⋆ *(Generalized quaternion groups)*
For $n \geq 3$, consider the generalized quaternion group:

$$Q_{2^n} := \langle i, j \mid i^{2^{n-2}} = j^2,\ iji = j\rangle.$$

Let V be a finite-dimensional $\mathbb{Q}$-vector space on which Q_{2^n} acts faithfully and linearly.

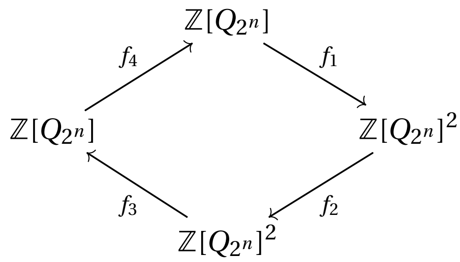
1. In this question, we aim at computing the group $\mathrm{Br}_{\mathrm{nr}}\overline{\mathbb{Q}}(V)^{Q_{2^n}}$ thanks to Bogomolov's formula.

12. With respect to Tate's perfect pairing of finite groups:

$$H^1(K_v,M)\times H^1(K_v,G^{\mathrm{ab}}) \to \mathrm{Br}(K_v) \subset \mathbb{Q}/\mathbb{Z}$$

given by the cup-product.

(a) Prove that the following square is exact:



where:

$$f_1 = \begin{pmatrix} i-1 \\ -(ij-1) \end{pmatrix}, \quad f_2 = \begin{pmatrix} \sum_{m=0}^{2^{n-2}-1} i^m & ij+1 \\ -(j+1) & i-1 \end{pmatrix}, \quad f_3 = \begin{pmatrix} i-1 & j-1 \end{pmatrix}, \quad f_4 = \sum_{x \in Q_{2^n}} x.$$

(b) Thanks to the previous question, compute the cohomology groups $H^*(Q_{2^n}, \mathbb{Z})$.

(c) Use Bogomolov's formula to compute $\mathrm{Br}_{\mathrm{nr}}\overline{\mathbb{Q}}(V)^{Q_{2^n}}$.

2. In this question, we aim at computing the group $\mathrm{Br}_{\mathrm{nr}_1}\mathbb{Q}(V)^{Q_{2^n}}$ thanks to Harari's formula. This computation is due to Demarche.

(a) Compute the group $Q_{2^n}^{\mathrm{ab}}$.

Let now p be an odd prime number and let $\mathbb{Q}_p^{\mathrm{tr}}$ be the maximal tamely ramified extension of $\mathbb{Q}_p$. Set $\Gamma_p := \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tr}}/\mathbb{Q}_p)$.

(b) Prove that, for each $b \in Q_{2^n}^{\mathrm{ab}}$, there exist elements $a_1, \dots, a_r, b_1, \dots, b_r \in Q_{2^n}$ such that the product $b_1 \dots b_r$ lifts b and $a_s b_s a_s^{-1} = b_s^p$ for each s.

(c) Deduce that the image of the natural map $\varphi : H^1(\Gamma_p, Q_{2^n}) \to H^1(\Gamma_p, Q_{2^n}^{\mathrm{ab}})$ spans the whole group $H^1(\Gamma_p, Q_{2^n}^{\mathrm{ab}})$.

Hint: recall that the group Γ_p is the profinite group generated by two elements σ and τ satisfying the relation $\sigma\tau\sigma^{-1} = \tau^p$.

(d) Deduce that the image of the natural map $H^1(\mathbb{Q}_p, Q_{2^n}) \to H^1(\mathbb{Q}_p, Q_{2^n}^{\mathrm{ab}})$ spans the whole group $H^1(\mathbb{Q}_p, Q_{2^n}^{\mathrm{ab}})$.

(e) Use Harari's formula to compute $\mathrm{Br}_{\mathrm{nr}_1}\mathbb{Q}(V)^{Q_{2^n}}$.

3. Compute the group $\mathrm{Br}_{\mathrm{nr}}\mathbb{Q}(V)^{Q_{2^n}}$ and use supersolvable descent to prove that the group Q_{2^n} satisfies the weak approximation property over $\mathbb{Q}$.

Remark: this result is not at all obvious, since for $n \geq 4$, the field $\mathbb{Q}(V)^{Q_{2^n}}$ is not rational.

Exercise 37: ⋆ *(Inverse Galois problem with norm conditions)*
Let K be a number field and $\mathscr{A} \subset K^\times$ a finitely generated subgroup. Let G be a supersolvable finite group. In this exercise, we are going to prove the following Theorem of Harpaz and Wittenberg: there exists a Galois extension L/K with Galois group G

such that every element of $\mathscr{A}$ is a norm from L. To do so, we choose an embedding $G \hookrightarrow \mathrm{SL}_n(K)$ and a finite system of generators $\alpha_1, \dots, \alpha_m \in \mathscr{A}$. We then consider the variety $Y := \mathrm{SL}_n \times T^{\alpha_1} \times \cdots \times T^{\alpha_m}$ where, for each α, we denote by T^α the fiber above α of the multiplication map $\prod_{g \in G} \mathbb{G}_\mathrm{m} \to \mathbb{G}_\mathrm{m}$. Note that G acts on the T^α's by permutation of the coordinates.

1. We make G act on Y diagonally and we set $X := Y/G$. It is well-known that the quotient $\mathrm{Br}_{\mathrm{nr}}(X)/\mathrm{Br}(K)$ is finite. Use Ekedahl's irreducibility Theorem [13] to prove that there exists $x \in X(K)$ such that the fiber Y_x is irreducible.
2. Conclude that the function field L of Y_x is a Galois extension of K with group G such that $\mathscr{A} \subset N_{L/K}(L^\times)$.

13. See Theorem 1.8 of the course notes.