NUMBER THEORETICAL TOPICS IN INVERSE GALOIS THEORY
–
EXERCISES AND PROBLEMS

PIERRE DÈBES

Problem 1 — *Show that every finite abelian group G is the Galois group of some field extension of $\mathbb{Q}$.*

Hints and comments — Consider first the special case that G is cyclic: use cyclotomic extensions and the lemma that for each integer $m \neq 0$, there are infinitely many integers that are congruent to 1 modulo m. (see [Dèb09, §2.1.2]).

Problem 2 — *Show that* 16 *is an* 8*th power in $\mathbb{Z}_p$ for every prime $p \neq 2$ and is not an* 8*th power in $\mathbb{Z}_2$.*

Hints and comments — Note that

$$X^8 - 16 = (X^2 - 2)(X^2 + 2)((X - 1)^2 + 1)((X + 1)^2 + 1)$$

This example shows that the local-global map

$$H^1(\mathbb{Q}, \mathbb{Z}/8\mathbb{Z}) \to \prod_{p \neq 2} H^1(\mathbb{Q}_p, \mathbb{Z}/8\mathbb{Z})$$

is not injective. It follows that the local-global map

$$H^2(\mathbb{Q}, \mathbb{Z}/8\mathbb{Z}) \to \prod_{p \neq 2} H^2(\mathbb{Q}_p, \mathbb{Z}/8\mathbb{Z})$$

is not surjective. More precisely, there is no Galois extension $E/\mathbb{Q}$ of group $\mathbb{Z}/8\mathbb{Z}$ such that the Frobenius at $p = 2$ is of order 8, or equivalently, such that $E\mathbb{Q}_2/\mathbb{Q}_2$ is unramified of degree 8.

Problem 3 — *Given a field k and a finite separable extension $F/k(T)$, show that the following assertions are equivalent:*
(i) $F \cap \overline{k} = k$,
(ii) *for every finite extension E/k,* $[FE : E(T)] = [F : k(T)]$,
(iii) $[F\overline{k} : \overline{k}(T)] = [F : k(T)]$.

Hints and comments — see [Dèb09, §2.3.1].

Date: July 12, 2015.

Problem 4 — *Show that for $k = \mathbb{Q}$, or more generally for a hilbertian field k, if a finite group G is a Galois group over $k(T)$, then it is a Galois group over k.*

Hints and comments — see [Dèb09, §2.2.4].

Problem 5 — *Let $F/k(T)$ be a degree n extension with F/k regular. Assume that the Galois closure $\widehat{F}/k(T)$ is of group S_n. Show that $\widehat{F}/k$ is regular. Give an example for which the conclusion fails if the assumption if removed.*

Problem 6 — Let G be a finite group and H be a subgroup of G. Denote by U the union of all conjugate subgroups gHg^{-1} of H by elements $g \in G$.

(a) Show that if $\{g_1, \dots, g_n\}$ are representatives of the left cosets of G modulo H, then $U \setminus \{1\} = \bigcup_{i=1}^{n} \left(g_i H g_i^{-1} \setminus \{1\}\right)$.

(b) Deduce that $\mathrm{card}(U) \leq |G| - [G : H] + 1$

(c) (*Jordan's lemma*) Let H be a subgroup of G that contains at least one element from each conjugacy class of G. Show that $H = G$.

(d) Let G be a transitive subgroup of S_n with $n > 1$. Show that there exists an element of G with no fixed point.

Problem 7 — *(Hensel's lemma)*

(a) *Show that $X^2 + 1$ has a root in $\mathbb{Z}_5 = \varprojlim_n \mathbb{Z}/5^n\mathbb{Z}$.*

(b) *Let (A, v) be a complete discrete valuation ring with residue field κ. Let $f \in A[X]$ be a polynomial such that the polynomial $\overline{f} \in \kappa[X]$ obtained by reducing the coefficients of f modulo the valuation ideal has a simple root $\lambda \in \kappa$. Show that f has a root $x \in A$.*

Hints and comments — see [Dèb09, §1.2.2.7].

Problem 8 — *Let $P \in \mathbb{Z}[Y]$ be a polynomial, irreducible in $\mathbb{Q}[Y]$. Show that there exist infinitely many primes p such that the polynomial P reduced modulo p has no roots in $\mathbb{F}_p$.*

Hints and comments — Use the classical density Tchebotarev theorem.

Problem 9 — *Let $P \in \mathbb{Z}[T, Y]$ be a polynomial, irreducible in $\overline{\mathbb{Q}(T)}[Y]$. Assume that the splitting field $\widehat{F}/\mathbb{Q}(T)$ of the polynomial P (in Y) is a regular Galois extension. Show that for all but finitely many primes p, the following property holds: there is a coset $p\mathbb{Z} + b \subset \mathbb{Z}$ such that for each $t_0 \in p\mathbb{Z} + b$, the polynomial $P(t_0, Y)$ has no root in $\mathbb{Q}$.*

Hints and comments — Use the function field Tchebotarev theorem.

Problem 10 — *Let* $\mathbf{t} \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ *be a finite subset, invariant under the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Set* $B^* = \mathbb{P}^1 \setminus \mathbf{t}$ *and let* p *be a prime number.*

(a) *Define the natural restriction map* $r_p : \pi_1(B^*, t)_{\mathbb{Q}_p} \to \pi_1(B^*, t)_{\mathbb{Q}}$.

(b) *Let* $F/\mathbb{Q}(T)$ *be a regular Galois extension of group* G *and* $\phi : \pi_1(B^*, t)_{\mathbb{Q}} \to G$ *be its fundamental group representation. Show that the map* $\phi \circ r_p : \pi_1(B^*, t)_{\mathbb{Q}_p} \to G$ *is a fundamental group representation of the regular Galois extension* $F\mathbb{Q}_p/\mathbb{Q}_p(T)$.

Problem 11 — *Let* $n \geq 1$ *be an integer and*

$$f(Y) = Y^n + a_1 Y^{n-1} + \cdots + a_n$$

be a polynomial with coefficients $a_i \in \mathbb{Q}$. *Set*

$$P(T, Y) = f(Y) - T$$

and denote by $\mathcal{Y} \in \overline{\mathbb{Q}(T)}$ *a root of the polynomial* $P(T, Y)$ *(in* Y*).*

(a) *Show that* $P(T, Y)$ *is irreducible in* $\overline{\mathbb{Q}}(T)[Y]$.

Set $E = \overline{\mathbb{Q}}(T)(\mathcal{Y})$, *denote the Galois closure of the extension* $E/\overline{\mathbb{Q}}(T)$ *by* $\widehat{E}/\overline{\mathbb{Q}}(T)$ *and its Galois group by* G.

(b) *Recall how* G *can be viewed as a transitive subgroup of* S_n.

From now on, assume that f *satisfies the following conditions:*

(i) The roots $\beta_1, \ldots, \beta_{n-1} \in \overline{\mathbb{Q}}$ *of the derivative* $f'(Y)$ *are simple.*

(ii) $f(\beta_i) \neq f(\beta_j)$ *for* $i \neq j$.

(c) *Show that the branch points of the extension* $E/\overline{\mathbb{Q}}(T)$ *are in the set* $\{f(\beta_1), \ldots, f(\beta_{n-1}), \infty\}$.

(d) *Show that for* $i = 1, \ldots, n-1$ *we have* $f(Y) - f(\beta_i) = (Y - \beta_i)^2 g_i(Y)$ *with* $g_i(Y) \in \overline{\mathbb{Q}}[Y]$ *separable and such that* $g_i(\beta_i) \neq 0$.

(e) *Show that, for* $i = 1, \ldots, n-1$, *there are* $n-2$ *unramified points and one ramified point in the extension* $E/\overline{\mathbb{Q}}(T)$ *above* $f(\beta_i)$, *and that every inertia group is generated by a* 2*-cycle.*

(f) *Show that if* $v_{1/T}$ *is the unique prolongation of the* $1/T$*-adic valuation from* $\overline{\mathbb{Q}}((1/T))$ *to the algebraic closure* $\overline{\overline{\mathbb{Q}}((1/T))}$, *then we have* $v_{1/T}(\mathcal{Y}) = -1/n$.

(g) *Show that, above* ∞, *there is a totally ramified point in the extension* $E/\overline{\mathbb{Q}}(T)$, *and that every inertia group is generated by a* n*-cycle.*

(h) *Denote by* R *the sum of all integers* $e(\mathcal{P}) - 1$ *where* $\mathcal{P}$ *ranges over all the points/places of* E *and* $e(\mathcal{P})$ *is the corresponding ramification index. Check that*

$$-2[E : \overline{\mathbb{Q}}(T)] + R = -2$$

(that is, via the Riemann-Hurwitz formula, the function field E is of genus 0) and that

$$E = \overline{\mathbb{Q}}(\mathcal{Y})$$

(that is, E a pure transcendental extension of $\overline{\mathbb{Q}}$).

(i) *Show that the group G is generated by the inertia groups above the points $f(\beta_1), \ldots, f(\beta_{n-1})$. Conclude that $G = S_n$ (by using that a transitive subgroup of S_n that is generated by 2-cycles (or, more generally by cycles of prime length) is equal to S_n).*

References

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

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

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