UNIVERSITÉ DE RENNES 1

Galois Theory

Exercises

Please do 10 exercises in the list below.

Exercise 1

What is the automorphism group of the field $\mathbb{Q}(\sqrt[3]{2})$? What are the field morphisms from $\mathbb{Q}(\sqrt[3]{2})$ to $\mathbb{C}$?

Exercise 2

Let p be a prime number, and let $L := \mathbb{F}_p(X)$ be the field of fractions of polynomials in one variable with coefficients in the finite field $\mathbb{F}_p$. Let $K := \mathbb{F}_p(X^p) \subseteq L$. What is the grouo of K-linear automorphisms of the field L?

Exercise 3

Let K be a field, and let $\overline{K}$ be an algebraic closure of K. Show that the extension $\overline{K}/K$ is normal. Is it separable?

Exercise 4

Let L/K and M/L be field extensions. Suppose that the extension M/K is normal. Show that the extension M/L is normal.

Exercise 5

Let Ω/K be a field extension, and let L_0, L_1 be two subfields of Ω containing K. Assume that the extensions L_0/K and L_1/K are normal. Show that the extensions $L_0 \cap L_1/K$ and L_0L_1/K are normal. (Here, L_0L_1 denotes the subfield of Ω generated by $L_0 \cup L_1$.)

Exercise 6

Prove that the extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are normal, and that $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal.

Exercise 7

Let K be a field, and $P(X) \in K[X]$. Let L be a splitting field of P over K. Prove that $[L : K] \leqslant (\deg P)!$.

Exercise 8

Prove that any finite extension is contained in a finite normal extension.

Exercise 9

Let p be a prime number, and let $L := \mathbb{F}_p(X, Y)$ be the field of fractions of polynomials in two variables over $\mathbb{F}_p$. Let $K := \mathbb{F}_p(X^p, Y^p) \subseteq L$. Prove that the degree of the extension L/K is p^2. Show that it is not a simple extension.

Exercise 10

Let L/K be a finite extension, and L_{sep} the subfield of elements of L separable over K. Denote by $[L : K]_s$ the number of K-linear field morphisms from L to an algebraic closure $\overline{K}$ of K. Prove that $[L : K]_s = [L_{\text{sep}} : K]$ and that $[L : K]_s$ divides $[L : K]$.

Exercise 11

Prove that any algebraic extension of a finite field is Galois.

Exercise 12

Let L/K be a finite Galois extension. Let G be a subgroup of $\mathrm{Gal}(L/K)$. Let $M := H^0(G, L)$. Let $\sigma \in \mathrm{Gal}(L/K)$. Prove that σM corresponds to the subgroup $\sigma G \sigma^{-1}$ by the Galois correspondence.

Exercise 13

Let q be some power of a prime number, and let $d \geqslant 1$ be an integer. Let $\varphi_q \colon \mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$ be the field automorphism defined by $\varphi_q(x) = x^q$. What are the minimal and characteristic polynomials of the $\mathbb{F}_q$-linear map φ_q.

Exercise 14

Let K be a field, and $n \geqslant 1$ an integer not divisible by the caracteristic of K. Let L be the extension of K generated by the n-th roots of unity. Denote by $\chi \colon \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ the cyclotomic character. Prove that the n-th cyclotomic polynomial Φ_n is irreducible if and only if χ is an isomorphism.

Exercise 15 : Carlyle circle

Let s and p be two algebraic real numbers. In $\mathbb{R}^2$, let $A := (0, 1)$ and $B := (s, p)$. Let $\mathcal{C}$ be the circle of diametre $[AB]$. Prove that the intersections of $\mathcal{C}$ and the line $\mathbb{R} \times \{0\}$ are the points $(x_0, 0)$ and $(x_1, 0)$, where x_0 and x_1 are the roots of the polynomial $X^2 - sX + p$. Explain how to make this construction with a compass only, starting with points of coordinates $(0, 0)$, $(1, 0)$, $(s, 0)$ and $(p, 0)$, when $p \neq -1$. Explain how to handle the case $p = -1$, for example by remplacing (s, p) with $(2s, 4p)$.

Exercise 16

Let L/K be a finite separable extension of degree n. Let M be an extension of K contening a Galois closure of L.

(i) Prove that there are exactly n K-linear field morphisms from L to M. These will be denoted by σ_0, ..., σ_{n-1} in the rest of the exercise.

(ii) Prove the existence of $x \in L$ such that $L = K[x]$.

(iii) Prove that 1, x, x^2, ..., x^{n-1} is a basis of L as a K-vector space.

(iv) What is the determinant of the matrix $(\sigma_i(x^j))_{0 \leqslant i,j < n}$? Prove that it is non-zero.

(v) Prove that the determinant of the matrix $(\mathrm{Tr}_{L/K}(x^{i+j}))_{0\leqslant i,j<n}$ is the square of the previous determinant. Deduce from this that $x, y \mapsto \mathrm{Tr}_{L/K}(xy)$ is a non-degenerate K-bilinear form on L.

(vi) Let $(e_j)_{0\leqslant j<n}$ be a basis of L as a K-vector space. Prove that the determinant of the matrix $(\sigma_i(e_j))_{0\leqslant i,j<n}$ is non-zero. Same question for the matrix $(\mathrm{Tr}_{L/K}(e_i e_j))_{0\leqslant i,j<n}$.

Exercise 17

Let L/K be a finite extension, and let $x \in L$. Prove that if L is not separable over K, then $\mathrm{Tr}_{L/K}(x) = 0$.

Exercise 18

Let M/L and L/K be finite extensions. Suppose that M/K is Galois. Using the formulas

$$\mathrm{Tr}_{M/K}(x) = \sum_{\sigma\in\mathrm{Gal}(M/K)} \sigma(x) \qquad \text{and} \qquad \mathrm{N}_{M/K}(x) = \prod_{\sigma\in\mathrm{Gal}(M/K)} \sigma(x),$$

prove that

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} \qquad \text{and} \qquad \mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}\,.$$

Exercise 19

Let G be a group acting on an A-module M. Denote by $Z^1(G, M)$ the set of 1-cocyles on G with values in M. Also denote by 1_G the neutral element of G, and by 0_M the neutral element of M. Let $c \in Z^1(G, M)$. Prove that $c_{1_G} = 0_M$.

Exercise 20

Let G be a group acting on an A-module M. Denote by $Z^1(G, M)$ the set of 1-cocyles on G with values in M, and $B^1(G, M)$ the set of 1-coboundaries on G with values in M. Prove that

$$B^1(G, M) \subseteq Z^1(G, M).$$

Exercise 21

Let G be a group, acting on a group H. Denote by

$$Z^1(G, H) \coloneqq \{c\colon G \to H / \forall \sigma, \tau \in G\ c_{\sigma\tau} = c_\sigma\, \sigma(c_\tau)\}\,.$$

the set of cocycles. Two cocycles c and c' are said to be cohomologous if there exists $x \in H$ such that

$$\forall \sigma \in G x c'_\sigma = c_\sigma \sigma(x).$$

Prove that this is an equivalence relation. Prove that if H is commutative, then this is the congruence relation modulo coboundaries.

Exercise 22

Let G be a cyclic group, and σ a generator. Assume that G acts on a commutative group M. Prove that the map

$$\begin{cases} H^1(G,M) & \longrightarrow & \operatorname{coker}(\mathrm{id}-\sigma) \\ c & \longmapsto & c_\sigma \end{cases}$$

is well defined, injective, and that its image is

$$\ker\left(\sum_{\tau\in G}\tau\right)\Big/\operatorname{im}(\mathrm{id}-\sigma)\ .$$

(Reminder: $\operatorname{coker}(\mathrm{id}-\sigma) := M/\operatorname{im}(\mathrm{id}-\sigma)$.)

Exercise 23

Let G be a group, H a subgroup of G, and M an $A[G]$-module. Prove that the map

$$\begin{cases} M & \longrightarrow & \mathrm{Ind}_H^G(M) \\ x & \longmapsto & (\sigma \mapsto \sigma(x)) \end{cases}$$

induces a morphism $H^1(G,M) \to H^1(G,\mathrm{Ind}_H^G(M))$. Using Shapiro's lemma, this yields a morphism $H^1(G,M) \to H^1(H,M)$. Prove that this is the restriction map.

Exercise 24

Describe and prove an analogue of Kummer's theory for abelian extensions of exposant p, in characteristic $p > 0$.

Exercise 25

Let $(X_i)_{i\in I}$ be a family of topological spaces. Denote by $\prod_{i\in I} X_i$ their product, and $\pi_j\colon \prod_{i\in I} X_i \to X_j$ the projection onto X_j, for every $j \in I$. Endow $\prod_{i\in I} X_i$ with the product topology, whose open subsets are the unions (not necessarily finite) of subsets $\prod_{i\in I} U_i$ where U_i is an open subset of X_i and $\{i \in I / U_i \neq X_i\}$ is finite. Prove that a sequence $(y^{(n)})_{n\geqslant 0}$ of elements of $\prod_{i\in I} X_i$ converges if and only if, for all i, $(\pi_i(y^{(n)}))_{n\geqslant 0}$ converges.

Exercise 26

Let K be a field, and $M \in \mathcal{K}_n(K)$. Prove that the K-algebra $K[M]$ is diagonalizable if and only if the matrix M is diagonalizable over K.

Exercise 27

Let K be a field, and $P(X) \in K[X]$. Prove that the K-algebra $K[X]/(P(X))$ is diagonalizable if and only if P is fully split, squarefree, over K.

Exercise 28

Prove that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is isomorphic to $\mathbb{C}^2$ as a $\mathbb{C}$-algebra, and describe explicitly the isomorphism.

Exercise 29

Let L/K be a finite extension of degree n. Prove that it is Galois if and only if the L-algebra $L \otimes_K L$ is isomorphic to L^n.

Exercise 30

Let K be a perfect field, and A a finite K-algebra. Prove that A is étale if and only if it is reduced (i.e. has no nilpotent element).

Exercise 31

Let A be commutative ring with unity, and S a subset of A, containing the unit element and stable under multiplication. Denote by $S^{-1}A$ the localized of A where the elements of S become invertible. Prove that there is an increasing (for the inclusion) bijection between the the prime ideals of $S^{-1}A$ and the prime ideals of A that do not intersect S.

Exercise 32

Let $K/\mathbb{Q}$ be the splitting field of $X^3 - 7$. Prove that its Galois group is isomorphic to $\mathfrak{S}_3$, and find every intermediate extension between $\mathbb{Q}$ and K.

Exercise 33

Prove that the fields $\mathbb{Q}(\sqrt{7})$ are $\mathbb{Q}(\sqrt{11})$ are not isomorphic.

Exercise 34

Let L/K be a finite extension of a finite field K. Prove that the trace $\mathrm{Tr}_{L/K}$ and norm $\mathrm{N}_{L/K}$ are surjective.

Exercise 35

Let L/K be a Galois extension of degree 8100. Prove that there is a field M, with $K \subseteq M \subseteq L$, such that the extension M/K has degree 100.