230C: Exercises on Galois theory

By: Michiel Kosters
Report mistakes to kosters@gmail.com

These exercises come from the UCI qualifying exams from $2009 - 2016$.

Exercise 1
Let $\zeta = e^{2\pi i/7} \in \mathbf{C}$ denote a primitive 7-th root of unity.
(a) True/False: Every element in $\mathbf{Q}(\zeta)$ can be expressed uniquely in the form

$$a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5 + a_6\zeta^6,$$

where $a_0, a_1, \ldots, a_6 \in \mathbf{Q}$. Briefly explain.
(b) Find the order of the element $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ induced by $\sigma : \zeta \to \zeta^2$. Briefly explain your answer.
(c) Find the degree of the field extension of $\mathbf{Q}(\zeta + \zeta^2 + \zeta^4)/\mathbf{Q}$. Explain your answer.

Exercise 2
True/False. For each of the following answer True or False and give a brief explanation.
(a) Every finite subgroup of $\mathrm{GL}_n(\mathbf{Q})$ is abelian.
(b) A finite extension of $\mathbf{Q}$ cannot have infinitely many distinct subfields.

Exercise 3
Let $L/\mathbf{Q}$ denote a Galois extension with Galois group isomorphic to A_4.
(a) Does there exist a quadratic extension $K/\mathbf{Q}$ contained in L? Prove your answer?
(b) Does there exist a degree 4 polynomial in $\mathbf{Q}[x]$ with splitting field equal to L? Prove your answer.

Exercise 4
For each of the following, either give an example or state that non exists. In either case, give a brief explanation.
(a) An element $\alpha \in \mathbf{Q}(\sqrt{2}, i)$ such that $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, i)$.
(b) A tower of field extensions $L \supseteq K' \supseteq K$ such that L/K' and K'/K are Galois extensions but L/K is not Galois.

Exercise 5
Construct a Galois extension F of $\mathbf{Q}$ satisfying $\mathrm{Gal}(F/\mathbf{Q}) \cong D_8$, the dihedral group of order 8. Fully justify.

Exercise 6
(a) Prove that $\mathbf{Q}(\sqrt[4]{T})$ is not Galois over $\mathbf{Q}(T)$, where T is an indeterminate.
(b) Find the Galois closure of $\mathbf{Q}(\sqrt[4]{T})$ over $\mathbf{Q}(T)$ and determine the Galois group both as an abstract group and as a set of explicit automorphisms. (Fully justify.)

Exercise 7
(a) What does it mean for a field to be perfect?
(b) Give an example of a perfect field. (No need to justify your answer.)
(c) Give an example of a field that is not perfect. (No need to justify your answer.)

Exercise 8
Determine the splitting field over $\mathbf{Q}$ of the polynomial $x^4 + x^2 + 1$, and the degree over $\mathbf{Q}$ of the splitting field.

Exercise 9
Let p be a prime. Prove that the Galois group for $x^p - 2$ over $\mathbf{Q}$ is isomorphic to the group of matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

with $a, b \in \mathbf{F}_p$, $a \neq 0$.

Exercise 10
Show that $\mathbf{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic extension of $\mathbf{Q}$, i.e., is a Galois extension of degree 4 with cyclic Galois group.

Exercise 11
Prove that every finite field is perfect, i.e., that every finite extension of a finite field is separable.

Exercise 12
Let E be the splitting field of $x^{21} - 1$ over $\mathbf{Q}$.
(a) What is the degree $[E : \mathbf{Q}]$?
(b) How many subfields does E have?

Exercise 13
Consider the extension of fields $\mathbf{R}(T) \subset \mathbf{R}(T^{1/4})$, where T is an indeterminate.
(a) Is $\mathbf{R}(T^{1/4})/\mathbf{R}(T)$ Galois? Why or why not?
(b) Find all intermediate fields F such that $\mathbf{R}(T) \subseteq F \subseteq \mathbf{R}(T^{1/4})$, and prove that you have found all of them.

Exercise 14
Let $f(x) \in \mathbf{Q}[x]$ be an irreducible cubic polynomial whose Galois group is denoted by G_f.
(a) Prove that if $f(x)$ has exactly one real root, then $G_f \cong S_3$.
(b) Find an irreducible cubic $f(x) \in \mathbf{Q}[x]$ whose roots generate the cubic subextension of $\mathbf{Q}(\zeta_7)/\mathbf{Q}$, where ζ_7 denotes a primitieve 7-th root of unity in $\mathbf{C}$.

Exercise 15
Let E be the splitting field of $x^{35} - 1$ over $\mathbf{F}_2$.
(a) How many elements does E have?
(b) How many subfields does E have?

Exercise 16
Suppose that F is a Galois extension of $\mathbf{Q}$ and let $\mathrm{Gal}(F/\mathbf{Q}) \cong S_4$. Show that there is an irreducible polynomial $g(x) \in \mathbf{Q}[x]$ of degree 4 such that the splitting field of $g(x)$ is F.

Exercise 17
Determine the Galois group of the splitting field of $x^3 + 2$ over $\mathbf{F}_3$, over $\mathbf{F}_7$, and over $\mathbf{F}_{11}$.

Exercise 18
For each of the following, either give an example or briefly explain why no such example exists:
(a) a quadratic extension of fields that is not separable.
(b) a nonabelian group in which all the proper subgroups are cyclic.
(c) an infinite field where every nonzero element has finite multiplicative order.
(d) a nonabelian group with trivial automorphism group.
(e) an element of order 4 in $\mathbf{R}/\mathbf{Z}$.

Exercise 19
Let $L = \mathbf{Q}(\sqrt[6]{-3})$. Show that $L/\mathbf{Q}$ is Galois and $\mathrm{Gal}(L/\mathbf{Q}) \cong S_3$.

Exercise 20
Show that $\sqrt[4]{2}$ is not contained in any field L that is Galois over $\mathbf{Q}$ with $\mathrm{Gal}(L/\mathbf{Q}) - S_n$, for any positive integer n. You may use without proof the fact that the Galois group of the polynomial $x^4 - 2$ over $\mathbf{Q}$ is the dihedral group of order 8.

Exercise 21
Let p be a prime and F an algebraically closed field of characteristic p. Let $n = p^a m$, where m is a positive integer not divisible by p. How many n-th roots of unity are there in F? Prove your answer.

Exercise 22
Determine the Galois closue F of the field $\mathbf{Q}(\sqrt{1+\sqrt{2}})$ over $\mathbf{Q}$. Determine all elements of the Galois group of the extension $F/\mathbf{Q}$ by describing their actions on the generators of F. Also describe G as an abstract group.

Exercise 23
Suppose F is a field and $f(x) \in F[x]$ is irreducible. Suppose that E is the splitting field over F for $f(x)$, and that for some $\alpha \in E$, we have $f(\alpha) = f(\alpha+1) = 0$. Show that the characteristic of F is not zero.

Exercise 24
Let p be an odd prime. Prove that $\mathbf{Q}(e^{2\pi i/p})$ contains a unique quadratic extension of $\mathbf{Q}$. For which p is this quadratic field contained in $\mathbf{R}$? Jusityf your answer.

Exercise 25
Let G be the Galois group of the polynomial $x^6 - 27$ over $\mathbf{Q}$. Determine all elements of G by describing their actions on the generators of the splitting field. Also describe G as an abstract group.

Exercise 26
Suppose F is a field of characteristic $p > 0$. Define a function $\phi : F \to F$ by $\phi(x) = x^p$.
(a) Show that ϕ is a field homomorphism.
(b) Show that if F is finite, then ϕ is an automorphism.
(c) Give an example of a field F usch that ϕ is not an automorphism.

Exercise 27
Let K/F be an algebraic extension of fields and let R be a ring such that $F \subseteq R \subseteq K$. Prove that R is a field.

Exercise 28
Determine the splitting field of $x^5 - 2$ over the finite field $\mathbf{F}_3$. Then determine the Galois group over $\mathbf{F}_3$ of $x^5 - 2$, both as an abstract group and as a set of automorphisms.

Exercise 29
Find the Galois group over $\mathbf{Q}$ of $x^3 + 4x + 2$, as an abstract group.

Exercise 30
Give an example of an extension of fields that is not separable. Compute its separable and inseparable degrees. (Fully justify your answers).

Exercise 31
Let n be a positive integer. Prove that the polynomial $f(x) = x^{2^n} + 8x + 13$ is irreducible over $\mathbf{Q}$.

Exercise 32
Determine the splitting field over $\mathbf{Q}$ of $x^4 - 2$. Then determine the Galois group over $\mathbf{Q}$ of $x^4 - 2$, both as an abstract group and as a set of automorphisms. Give the lattice of subgroups and the lattice of subfields. Make clear which subfield is the fixed field of which subgroup.

Exercise 33
(a) Give an example of an infinite group in which every element has finite order.
(b) How many solutions does the equation $x^n + \ldots + x + 1 = 0$ have in a finite field $\mathbf{F}_q$?

Exercise 34
Suppose that F is an algebraically closed field. Find all monic separable polynomials $f \in F[x]$ such that the set of zeros of f in F is closed under multiplication.

Exercise 35
Compute the Galois group of the polynomial $f(x) = x^5 - 4x + 2$ over $\mathbf{Q}$.

Exercise 36
Prove that the Galois group of the polynomials $x^5 - 2$ over $\mathbf{Q}$ is isomorphic to the group of all matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

where $a, b \in \mathbf{F}_5$ and $a \neq 0$.

Exercise 37
Let $\mathbf{F}_q$ be a finite field of q elements. Show that every element $x \in \mathbf{F}_q$ can be

written as the sum of two squares in $\mathbf{F}_q$, that is, $x = y^2 + z^2$ for some $y, z \in \mathbf{F}_q$.