Galois theory — Exercise sheet 1

https://www.maths.tcd.ie/~mascotn/teaching/2023/MAU34101/index.html

Version: September 26, 2023

Submit your answers by Friday October 6, 4PM.

Instructions: **Only exercises 3 and 4 are mandatory; you must submit your answers to them before the deadline. The other exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercises. More specifically, Exercises 1 and 2 are revisions which may help you to solve the mandatory exercises; Exercise 5 is extra revisions, and Exercise 6 is an actual exercise on the contents of chapter 1.**

Exercise 1 *Revisions: Irreducible polynomials of low degree*

1. Let K be a field, and let $F(x) \in K[x]$ have degree 2 or 3. Prove that $F(x)$ is irreducible over K if and only if $F(x)$ has no root in K.

   Note: Irreducible over K is a synonym for irreducible in $K[x]$.

2. Exhibit a counter-example to show that the previous statement is no longer true if $\deg F \geqslant 4$. Does one of the implications remain true, or can both directions fail?

Exercise 2 *Revisions: Quotients and morphisms*

Let R and S be rings, let I be an ideal of R, let J be an ideal of S, and let $f : R \longrightarrow S$ be a ring morphism. Give a necessary and sufficient condition for f to induce a well-defined ring morphism from R/I to S/J.

Exercise 3 *Small non-prime finite fields (50 pts)*

1. (10 pts) Make a complete list of all finite fields (up to isomorphism) with at most 30 elements and which are not isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p \in \mathbb{N}$.

2. (30 pts) Give an explicit construction for each of them.

3. (10 pts) Make a list of all pairs (K, L) such that K and L are in your list and that L contains a copy of K (up to isomorphism).

Exercise 4 *Two models for $\mathbb{F}_8$ (50 pts)*

Let $K = \mathbb{F}_2[x]/(x^3 + x + 1)$ and $L = \mathbb{F}_2[y]/(y^3 + y^2 + 1)$.

1. (5 pts) Prove that K and L are fields.

2. (15 pts) Determine the number of elements of K, and of L. Why does your answer imply that K and L are isomorphic?

3. (30 pts) Describe explicitly an isomorphism between K and L.

   Hint: Which equation does the class of $y + 1 \in L$ satisfy? (Remember that $z = -z$ in characteristic 2, since $2z = 0$.)

Exercise 5 *Revisions: Square roots*

1. Let K be a field of characteristic different from 2, and let L be an extension of K of degree 2. Prove that $L = K(\sqrt{a})$ for some $a \in K$, meaning that $L = K(\alpha)$ for some $\alpha \in L$ such that $\alpha^2 \in K$.

   Hint: The quadratic formula $\frac{-b \pm \sqrt{\Delta}}{2a}$ is valid in any characteristic other than 2 (but not in characteristic 2, as it would make us divide by $2 = 0$).

2. Let still K be a field of characteristic different from 2. We say that an element $c \in K$ is a square in K if there exists $d \in K$ such that $c = d^2$.

   Let $a, b \in K^\times$, and let $\sqrt{a}, \sqrt{b}$ denote one of their square roots in some algebraic closure of K. Prove that $K(\sqrt{a}) = K(\sqrt{b})$ if and only if a/b is a square in K.

3. Use the previous questions to find all extensions of degree 2 of $\mathbb{R}$.

4. Let $r = n/d \in \mathbb{Q}^\times$ be a nonzero rational number, where $n \in \mathbb{Z}$, $d \in \mathbb{Z}_{\geqslant 1}$, and $\gcd(n, d) = 1$. Prove that r is a square in $\mathbb{Q}$ iff. n and d are squares in $\mathbb{N}$.

   Hint: Recall that each positive integer can be factored uniquely *into a product of primes, and that each rational number can be written* uniquely *as n/d with $n \in \mathbb{Z}$, $d \in \mathbb{Z}_{\geqslant 1}$, and $\gcd(n, d) = 1$.*

5. Justify carefully that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Determine $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) : \mathbb{Q}]$.

Exercise 6 *Splitting fields*

The two questions of this exercise are independent from each other.

Let K be a field, let $F(x) \in K[x]$ have degree $n \geqslant 1$, and let $\alpha_1, \cdots, \alpha_n$ be the roots of $F(x)$ in an algebraic closure $\overline{K}$ of K, ordered in some arbitrary way.

1. Prove that $K(\alpha_1, \cdots, \alpha_{n-1})$ is a splitting field of $F(x)$ over K.

   Hint: What is $\alpha_1 + \cdots + \alpha_n$?

2. Let L be a splitting field of $F(x)$ over K. Prove that $[L : K] \leqslant n!$.