Galois theory — Exercise sheet 1

https://www.maths.tcd.ie/~mascotn/teaching/2025/MAU34101/index.html

Version: October 3, 2025

Deadline: Monday October 13, 2PM.
Either bring your answers to class, or email them to the TA.

Instructions: **Only exercises 1, 2, and 3 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.**

Exercise 1 *Revisions: Irreducible polynomials of low degree (10 pts)*

1. (5 pts) 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. (5 pts) Exhibit a counter-example to show that the previous statement is no longer true if $\deg F = 4$. Does one of the implications remain true, or can both directions fail?

Exercise 2 *Embeddings of stem fields (45 pts)*

Let K be a field, $P(x) \in K[x]$ irreducible over K, $L = K[x]/(P(x))$ the "standard" stem field of $P(x)$ over K, and finally let M be another field extension of K.

We will denote the class of a polynomial $F(x) \in K[x]$ in L as $\overline{F(x)}$. In particular, $\bar{x}$ is the class of x in L, which is a root of $P(x)$ in L, and $\overline{F(x)} = F(\bar{x})$.

1. (10 pts) Suppose there exists a K-morphism $f : L \to M$. Prove that $f(\bar{x}) \in M$ is a root of $P(x)$.

2. (20 pts) Conversely, suppose that $\mu \in M$ is a root of $P(x)$. Prove that

$$f_\mu : \begin{array}{ccc} L & \longrightarrow & M \\ \overline{F(x)} & \longmapsto & F(\mu) \end{array}$$

   is well-defined, and is a K-morphism from L to M.

   Hint: Consider the "evaluate at $x = \mu$" map $\mathrm{ev}_\mu : \begin{array}{ccc} K[x] & \longrightarrow & M \\ F(x) & \longmapsto & F(\mu) \end{array}$.

3. (15 pts) Deduce that the sets $F = \mathrm{Hom}_K(L, M)$ of K-morphisms from L to M is in 1-to-1 correspondence with the set $R = \{\mu \in M \mid P(\mu) = 0\}$ of roots of $P(x)$ in M. Write down explicitly bijections $\phi : F \longrightarrow R$ and $\psi : R \longrightarrow F$ which are inverses of each other.

Exercise 3 *Two models for $\mathbb{F}_8$ (45 pts)*

Recall that $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Let $A(x) = x^3+x^2+1 \in \mathbb{F}_2[x]$ and $B(x) = x^3+x+1 \in \mathbb{F}_2[x]$.

Define $L = \mathbb{F}_2[x]/(A(x))$ and $M = \mathbb{F}_2[x]/(B(x))$.We will write α for the class of x in K, and β for the class of x in L; thus $\alpha^3+\alpha^2+1 = 0 = \beta^3+\beta+1$.

1. (10 pts) Prove that L and M are fields.
2. (8 pts) Determine the number of elements of L, and of M, and list their elements.

   Hint: What is the minimal polynomial of α over $\mathbb{F}_2$?
3. (5 pts) Why does your answer to the previous question imply that L and M are isomorphic as fields?
4. (2 pts) Prove that any field morphism from L to M is automatically an $\mathbb{F}_2$-morphism.
5. (20 pts) Describe explicitly an isomorphism between L and M, by specifying the image of every single element of L.

   Hint: Use Exercise 2. Also remember that in charaterestic 2, since $2x = 0$, we have $x = -x$ and $(x+y)^2 = x^2+y^2$; so, in your computations, you can ignore signs, and compute squares of sums as sums of squares.

Exercise 4 *Fields of distinct characteristic belong in separate universes*

Let L and M be two fields, and suppose that there exists a field morphism f from L to M.

1. Prove that L and M have the same characteristic.

   Hint: Consider ring morphisms from $\mathbb{Z}$.
2. Let K_0 be the prime subfield of L. Prove that K_0 is also the prime subfield of M.
3. Prove that f is automatically a K_0-morphism.

Exercise 5 *Small non-prime finite fields*

1. 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. Give an explicit construction for each of them.
3. 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 6 *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 7 *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 $[L : K] \leqslant n!$.

Exercise 8 *A formula for the discriminant*

Let $F(x) = x^n + bx + c \in \mathbb{C}[x]$, where $n \geqslant 2$ and $b, c \in \mathbb{C}$. Let $\beta \in \mathbb{C}$ be such that $\beta^{n-1} = -b/n$, and let $\zeta = e^{2\pi i/(n-1)}$, so that $\zeta^{n-1} = 1$ and that $x^{n-1} - y^{n-1} = \prod_{k=0}^{n-2}(x - \zeta^k y)$.

1. Express the roots of $F'(x)$ in terms of ζ and β.

2. Prove that $F(\zeta^k\beta) = \left(1 - \frac{1}{n}\right)\beta\zeta^k b + c$ for all $k \in \mathbb{Z}$.

3. Deduce that $\operatorname{disc} F = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big)$.

4. For which primes $p \in \mathbb{N}$ does the polynomial $x^5 - 5x + 6$ have multiple roots in $\overline{\mathbb{F}_p}$?