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?

Solution 1

1. If $x_0 \in K$ is a root of F, then $x - x_0 \in K[x]$ is a non-constant factor of $F(x)$, so we have $F(x) = (x - x_0)G(x)$ for some $G(x) \in K[x]$ of degree $\deg G = \deg F - 1 \geqslant 1$. So neither $x - x_0$ nor $G(x)$ are constant, so their are not invertible in the ring $K[x]$, so $F(x) = (x - x_0)G(x)$ is a "genuine" factorisation which shows that F is reducible over K if it has a root in K. Note that this implication remains valid even if $\deg F \geqslant 4$.

   Conversely, suppose $F(x)$ is reducible over K. Then we can write $F(x) = A(x)B(x)$ with $A(x), B(x) \in K[x]$ non-constant (since constant polynomials are invertible in the ring $K[x]$, and therefore do not count as "true" factors). If $\deg A = 1$, say $A(x) = a_1x + a_0$ with $a_0, a_1 \in K$ and $a_1 \neq 0$, then $x = -a_0/a_1 \in K$ is a root of $A(x)$, and therefore of $F(x)$. Similarly, if $\deg B = 1$, then $B(x)$ and therefore $F(x)$ have a root in K. Finally, either $\deg A = 1$ or $\deg B = 1$ (or both), since otherwise $\deg F = \deg A + \deg B \geqslant 2 + 2 = 4$ whereas we assumed $\deg F \leqslant 3$. So if F is reducible, then F has a root in K.

2. We have already mentioned that any polynomial of degree at least 2 must be reducible over K if it has a root in K, so this implication survives.

However, the converse is no longer true: a polynomial of degree 4 or more may be reducible over K even if it does not have a root in K, because it could be the product of several irreducible factors all of degree 2 or more, in which case it won't have roots in K as these factors cannot have roots in K since otherwise they would be reducible over K. For instance, $F(x) = (x^2+1)(x^2+2)$ is clearly reducible over $K = \mathbb{R}$, even though it has no roots in $\mathbb{R}$ since it is positive everywhere.

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.

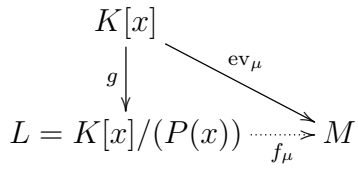
Hint: Consider the "evaluate at $x = \mu$" map $\mathrm{ev}_\mu : \begin{array}{ccc} K[x] & \longrightarrow & M \\ F(x) & \longmapsto & F(\mu) \end{array}$.

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.

Solution 2

1. Since f is a K-morphism, it preserves "rootness" of polynomials with coefficients in K, i.e. for all $F(x) \in K[x]$, f takes roots of $F(x)$ in L to roots of $F(x)$ in M. The results follows by taking $F(x) = P(x)$, as $\bar{x} \in L$ is a root of $P(x)$.

2. Consider the diagram



where ev_μ is as in the hint and g is the canonical projection coming form the fact that L is a quotient of $K[x]$. Both g and ev_μ are ring morphisms, and ev_μ will descent into a well-defined ring morphism f_μ if and only if the ideal

$(P(x))$ that we quotient by to get L is mapped to $0 \in M$ by ev_μ (so that the image of an equivalence class is not ambiguous; this is an avatar of the isomorphism theorem for rings). But in our case, the elements of $(P(x))$ are the multiples $P(x)G(x)$, $G(x) \in K[x]$ of $P(x)$; and those get mapped by ev_μ to $P(\mu)G(\mu) = 0$ since μ is a root of $P(x)$. Thus f_μ is a well-defined ring morphism.

Since L and M are fields, f_μ is actually a field morphism. Since $\mathrm{ev}_\mu \mathrm{R}$ is the identity on constant polynomials, f_μ is the identity on K, i.e. is a K-morphism, as desired.

3. Let
$$\phi : \begin{array}{ccc} F & \longrightarrow & R \\ f & \longmapsto & f(\bar{x}), \end{array}$$
which is well-defined since, by question 1., $f(\bar{x}) \in M$ is indeed a root of $P(x)$; and let
$$\psi : \begin{array}{ccc} R & \longrightarrow & F \\ \mu & \longmapsto & f_\mu, \end{array}$$
which is well-defined since, by question 2., f_μ is a well-defined element of F.

Let us check that ϕ and ψ are inverses of each other (which will of course imply that they are both bijective).

For each $\mu \in R$, we have indeed $\phi(\psi(\mu)) = \phi(f_\mu) = f_\mu(\bar{x}) = \mu$ by definition of f_μ as the map induced by ev_μ (i.e. the polynomial x evaluated at $x = \mu$ is μ). Thus $\phi \circ \psi = \mathrm{Id}_R$.

Let now $f \in F$ be a K-morphism from L to M, and let $\mu_f = \phi(f) = f(\bar{x}) \in R$. In order to prove that $\psi \circ \phi = \mathrm{Id}_F$, we need to check that $f = f_{\mu_f}$. We already know that f and f_{μ_f} agree on $\bar{x} \in L$, since $f_{\mu_f}(\bar{x}) = \mu_f = f(\bar{x})$. But then, since the K-morphisms f and f_{μ_f} agree on the generator $\bar{x}$ of $L = K[x]/(P(x)) = K[\bar{x}]$, they must be equal: for all $G(x) = \sum_n g_n x^n \in K[x]$, the fact that f is a K-morphism shows that
$$f\big(\overline{G(x)}\big) = \sum_n f(\overline{g_n x_n}) = \sum_n f(\overline{g_n}) f(\bar{x})^n \underset{g_n \in K}{=} \sum_n g_n \mu_f^n = G(\mu_f) = f_{\mu_f}\big(\overline{G(x)}\big);$$
thus $f = f_{\mu_f}$ as claimed.

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.

Solution 3

1. We need to prove that $A(x)$ and $B(x)$ are irreducible over $\mathbb{F}_2$. As they have degree 3, we can invoke Exercise 1, which shows that we just need to check that they have no roots in $\mathbb{F}_2$. But $\mathbb{F}_2 = \{0, 1\}$, so this means we just need to ensure that they do not vanish at 0 nor at 1, which is easy.

2. As $A(x)$ is monic and irreducible over $\mathbb{F}_2$, it is the minimal polynomial of α over $\mathbb{F}_2$; therefore we have that each element of K is *uniquely* of the form $a_0+a_1\alpha+\cdots a_{\deg A-1}\alpha^{\deg A-1} = a_0+a_1\alpha+a_2\alpha^2$ for some $a_0, a_1, a_2 \in \mathbb{F}_2 = \{0, 1\}$.

   Thus $K = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$, where these elements are pairwise distinct by uniqueness; in particular, K has exactly 8 elements.

   The exact same logic shows that $B(x)$ is the minimal polynomial of β over $\mathbb{F}_2$, whence $L = \{0, 1, \beta, \beta + 1, \beta^2, \beta^2 + 1, \beta^2 + \beta, \beta^2 + \beta + 1\}$ also has 8 elements.

3. Since K and L are two finite fields of the same cardinal, they must be isomorphic by the theorem seen in class.

4. Let $f : L \longrightarrow M$ be a field morphism. As $\mathbb{F}_2 = 0, 1$, we have $f(x) = x$ for all $x \in \mathbb{F}_2$, so f is actually an $\mathbb{F}_2$-morphism. Alternatively, invoke Exercise 4.

5. Any field morphism from L to M will be injective, and thus an isomorphism by cardinals. Furthermore, by the previous question, there is no loss of generality in searching for a morphism from L to M which is actually an $\mathbb{F}_2$-morphism. But since $L = \mathbb{F}_2[x]/(A(x))$, Exercise 2 informs us that such $\mathbb{F}_2$-morphisms correspond to roots of $A(x)$ in M. In particular, there must be at least one such root, since we know there is at least one such morphism.

   Let us thus search for a root μ of $A(x)$ in $M = \{0, 1, \beta, \beta + 1, \beta^2, \beta^2 + 1, \beta^2 + \beta, \beta^2+\beta+1\}$. After a few attempts, we find that $\mu = \beta+1$ satisfies $\mu^2 = \beta^2+1$ whence $\mu^3 = (\beta + 1)(\beta^2 + 1) = \beta^3 + \beta^2 + \beta + 1 = \beta^2$, which shows that μ is a root of $A(x)$. We thus obtain the isomorphism $f = f_\mu : L \longrightarrow M$ mapping

$\alpha = \bar{x}$ to $\mu = \beta + 1$. Explicitly:

$$\begin{aligned} 0 &\mapsto 0 \\ 1 &\mapsto 1 \\ \alpha &\mapsto \beta + 1 \\ \alpha + 1 &\mapsto \beta \\ \alpha^2 &\mapsto \beta^2 + 1 \\ \alpha^2 + 1 &\mapsto \beta^2 \\ \alpha^2 + \alpha &\mapsto \beta^2 + \beta \\ \alpha^2 + \alpha + 1 &\mapsto \beta^2 + \beta + 1. \end{aligned}$$

Remark. *We will see that* $\mathrm{Aut}(L)$ *and* $\mathrm{Aut}(M)$ *are cyclic of order 3 and generated by* $\mathrm{Frob} : x \mapsto x^2$. *Therefore, there are actually 3 isomorphisms from* L *to* M. *As we have seen, they are in 1-to-1 correspondence with the roots of* $A(x)$ *in* M, *so there are 3 such roots, which are the three Galois conjugates of* μ, *namely* $\mu = \beta + 1$, $\mathrm{Frob}(\mu) = \mu^2 = \beta^2 + 1$, *and* $\mathrm{Frob}^2(\mu) = (\beta^2 + 1)^2 = \beta^4 + 1 = \beta^2 + \beta + 1$, *whence the 3 isomorphisms* $F(\alpha) \mapsto F(\beta + 1),\ F(\beta^2 + 1),\ F(\beta^2 + \beta + 1)$ *from* L *to* M.

Thus the other two isomorphisms are explicitly

$$\begin{aligned} 0 &\mapsto 0 \\ 1 &\mapsto 1 \\ \alpha &\mapsto \beta^2 + 1 \\ \alpha + 1 &\mapsto \beta^2 \\ \alpha^2 &\mapsto \beta^2 + \beta + 1 \\ \alpha^2 + 1 &\mapsto \beta^2 + \beta \\ \alpha^2 + \alpha &\mapsto \beta \\ \alpha^2 + \alpha + 1 &\mapsto \beta + 1. \end{aligned}$$

and

$$\begin{aligned} 0 &\mapsto 0 \\ 1 &\mapsto 1 \\ \alpha &\mapsto \beta^2 + \beta + 1 \\ \alpha + 1 &\mapsto \beta^2 + \beta \\ \alpha^2 &\mapsto \beta + 1 \\ \alpha^2 + 1 &\mapsto \beta \\ \alpha^2 + \alpha &\mapsto \beta^2 + 1 \\ \alpha^2 + \alpha + 1 &\mapsto \beta^2. \end{aligned}$$

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.

Solution 4

1. We saw in class that each ring R admits a *unique* ring morphism $i_R : \mathbb{Z} \longrightarrow R$. By uniqueness, the ring morphisms i_M and $f \circ i_L$ from $\mathbb{Z}$ to M thus agree. Since f, being a field morphism, is automatically injective, we deduce that $\operatorname{Ker} i_L = \operatorname{Ker} i_M$. As $\operatorname{char} R$ is defined in terms of $\operatorname{Ker} i_R$, the result follows.

   Remark 1: By contrapositive, this shows that $\operatorname{Hom}(L, M) = \emptyset$ *when* $\operatorname{char} L \neq \operatorname{char} M$*, whence the name of the Exercise.*

   Remark 2: This does NOT generalise to rings! For example, we have an obvious morphism $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ from characteristic 0 to characteristic n. The difference with the field case is that ring morphisms need not be injective. We can still deduce that if there exists a ring morphism $f : R \longrightarrow S$, then $\operatorname{char} S \mid \operatorname{char} R$.

2. We saw in class that the prime subfield of a field only depends on the characteristic of that field (it is $\mathbb{Q}$ in characteristic 0, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ in characteristic $p > 0$). Thus L and M have the same prime subfield K_0 by the previous question.

3. This common prime subfield is the subfield generated by 0 and 1 (or even by $\emptyset$, since any field must contain 0 and 1). Thus the field morphisms f and Id, which agree on this generating set, must agree on the whole of K_0. This shows that f is 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).

Solution 5

1. Finite fields are determined up to isomorphism by their cardinal, which can be any prime power. Since we exclude prime, our list consists in

$$\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_9, \mathbb{F}_{16}, \mathbb{F}_{25}, \mathbb{F}_{27},$$

which are respectively extensions of

$$\mathbb{F}_2, \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_2, \mathbb{F}_5, \mathbb{F}_3$$

of degree

$$2, 3, 2, 4, 2, 3.$$

2. To construct them explicitly, we need irreducible polynomials of appropriate degrees over the appropriate $\mathbb{F}_p$. In all cases but $\mathbb{F}_{16}$, we can invoke Exercise 1.

$$x^2{+}x{+}1 \text{ has no roots in } \mathbb{F}_2 \Longrightarrow \text{irreducible over } \mathbb{F}_2 \Longrightarrow \mathbb{F}_4 \simeq \mathbb{F}_2[x]/(x^2{+}x{+}1),$$

$$x^2 + 1 \text{ has no roots in } \mathbb{F}_3 \Longrightarrow \text{irreducible over } \mathbb{F}_3 \Longrightarrow \mathbb{F}_9 \simeq \mathbb{F}_3[x]/(x^2 + 1),$$

$$x^2 + 2 \text{ has no roots in } \mathbb{F}_5 \Longrightarrow \text{irreducible over } \mathbb{F}_5 \Longrightarrow \mathbb{F}_{25} \simeq \mathbb{F}_5[x]/(x^2 + 2).$$

A polynomial of degree 3 either factors as $1 + 1 + 1$, $2 + 1$, or is irreducible; in particular, if it has no root, then it is irreducible. We thus find

$$x^3{+}x{+}1 \text{ has no roots in } \mathbb{F}_2 \Longrightarrow \text{irreducible over } \mathbb{F}_2 \Longrightarrow \mathbb{F}_8 \simeq \mathbb{F}_2[x]/(x^3{+}x{+}1),$$

$$x^3{-}x{+}1 \text{ has no roots in } \mathbb{F}_3 \Longrightarrow \text{irreducible over } \mathbb{F}_3 \Longrightarrow \mathbb{F}_{27} \simeq \mathbb{F}_3[x]/(x^3{-}x{+}1).$$

Finally, a polynomial of degree 4 either factors as $1 + 1 + 1 + 1$, $2 + 1 + 1$, $3 + 1$, $2 + 2$, or is irreducible; in particular, if it has no root, then either it is irreducible or it factors as $2 + 2$. However we find that the only irreducible of degree 2 over $\mathbb{F}_2$ is $x^2 + x + 1$, and $x^4 + x + 1 \neq (x^2 + x + 1)^2 = x^4 + x^2 + 1$ and has no roots, so it is irreducible, whence

$$\mathbb{F}_{16} \simeq \mathbb{F}_2[x]/(x^4 + x + 1).$$

Remark. *These are not the only possible choices of irreducible polynomials, and therefore not the only possible choices of models for these finite fields. See the next exercise for an example.*

3. We know that $\mathbb{F}_q \subset \mathbb{F}_{q'}$ iff. $q'$is a power of q. Therefore, the only inclusions between fields in our list is $\mathbb{F}_4 \subset \mathbb{F}_{16}$.

Remark. *We will see later that* $\mathbb{F}_4$ *has a nontrivial automorphism of order* 2*, so that there are actually* two *distinct embeddings of* $\mathbb{F}_4$ *into* $\mathbb{F}_{16}$*.*

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 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) : \mathbb{Q}]$.

Solution 6

1. $[L : K] \neq 1$ so $L \supsetneq K$, so let $\alpha \in L \setminus K$. Then $K \subsetneq K(\alpha) \subseteq L$, so by the tower law, $2 = [L : K] = [L : K(\alpha)][K(\alpha) : K]$. As $[K(\alpha) : K] > 1$ since $\alpha \notin K$, we conclude that $[L : K(\alpha)] = 1$, so $L = K(\alpha)$.

   Furthermore, since L/K is finite, α is algebraic over K, of degree $[K(\alpha) : K] = 2$. Let $m(x) \in K[x]$ be its minimal polynomial; it is monic, irreducible, and of degree 2, say $m(x) = x^2 + bx + c$ (we are actually not going to use irreducibilty in what follows). Then by the quadratic formula, $\alpha = \frac{-b \pm \sqrt{\Delta}}{2}$, where $\Delta = b^2 - 4c \in K$. This shows that $\alpha \in K(\sqrt{\Delta})$, so $K(\alpha) \subseteq K(\sqrt{\Delta})$. But we can also solve for $\sqrt{\Delta}$ and write $\sqrt{\Delta} = \pm(2\alpha + b)$, whence $\sqrt{\Delta} \in K(\alpha)$ so $K(\sqrt{\Delta}) \subseteq K(\alpha)$. In conclusion, $K(\sqrt{\Delta}) = K(\alpha) = L$.

   Remark: This is NOT true in higher degrees; for instance, "most" extensions of $\mathbb{Q}$ of degree 3 are NOT of the form $\mathbb{Q}(\sqrt[3]{r})$ for any $r \in \mathbb{Q}$. This is because the formula to solve equations of degree 3 is much more complicated than the quadratic formula (not to mention that in degree 5 and higher, there simply isn't any formula).

2. Observation: nonzero squares in K form a *subgroup* of $K^\times$.

   - Suppose first that a is a square in K. Then $\sqrt{a} \in K$, so $K(\sqrt{a}) = K$. Therefore, if b is also a square in K, then

     $$K(\sqrt{a}) = K = K(\sqrt{b});$$

     whereas if b is not a square in K, then

     $$K(\sqrt{a}) = K \subsetneq K(\sqrt{b}).$$

So the equivalence is satisfied in these cases.

- Suppose now that a is not a square in K. Then $x^2 - a \in K[x]$ is of degree 2 and rootless in K, so it is irreducible over K (see Exercise 1). As it is monic, it is the minimal polynomial of $\sqrt{a}$ over K, so $[K(\sqrt{a}) : K] = 2$ and $(\sqrt{a}^n)_{0 \leqslant n < 2}$ is a K-basis of $K(\sqrt{a})$, so each element of $K(\sqrt{a})$ is of the form $u(\sqrt{a})^0 + v(\sqrt{a})^1 = u + v\sqrt{a}$ for some *unique* $u, v \in K$.

  So if $K(\sqrt{a}) = K(\sqrt{b})$, then $\sqrt{b} \in K(\sqrt{a})$, so $\sqrt{b} = u + v\sqrt{a}$ for some $u, v \in K$. Squaring yields $b = (u^2 + av^2) + 2uv\sqrt{a}$. Both we also have $b = b1 + 0\sqrt{a}$, so by uniqueness,$u^2 + av^2 = b$ and $2uv = 0$. As $\operatorname{char} K \neq 2$ by assumption, $2 \neq 0$ in K, so $u = 0$ or $v = 0$. If $v = 0$, then $u^2 = b$; but then b is a square in K so $K(\sqrt{b}) = K \subsetneq K(\sqrt{a})$, absurd. Therefore $u = 0$, so $av^2 = b$, so $v \neq 0$ as $b \neq 0$, whence $a/b = (1/v)^2$ is a square in K.

  Conversely, suppose that a/b is a square in K, say $a/b = r^2$ where $r \in K^\times$. Then $\sqrt{b} = \pm r\sqrt{a} \in K(\sqrt{a})$ so $K(\sqrt{b}) \subseteq K(\sqrt{a})$, and $\sqrt{a} = \pm\frac{1}{r}\sqrt{b} \in K(\sqrt{b})$ so $K(\sqrt{a}) \subseteq K(\sqrt{b})$, whence $K(\sqrt{a}) = K(\sqrt{b})$.

Remark: This criterion is only useful if we have a good test for squareness in K. See next question for $K = \mathbb{R}$, and the question after that for $K = \mathbb{Q}$.

3. Observation: An element of $\mathbb{R}$ is a square in $\mathbb{R}$ if and only if it is nonnegative.

   Let L be an extension of $\mathbb{R}$ of degree 2. As $\operatorname{char} \mathbb{R} = 0 \neq 2$, the first question applies and shows that $L = \mathbb{R}(\sqrt{a})$ for some $a \in \mathbb{R}$. If $a \geqslant 0$, then $\sqrt{a} \in \mathbb{R}$, so $L = \mathbb{R}$, absurd. Therefore $a < 0$. But then $a = (-1)(-a)$ where $-a > 0$ is a square in $\mathbb{R}$, so $\mathbb{R}(\sqrt{a}) = \mathbb{R}(\sqrt{-1})$ by the previous question. Therefore the only possibility is $L = \mathbb{R}(\sqrt{-1}) = \mathbb{C}$.

4. Clearly, if $n = m^2$ and $d = e^2$ are squares in $\mathbb{N}$, then $r = (m/e)^2$ is a square in $\mathbb{Q}$. Conversely, suppose r is a square in $\mathbb{Q}$, say $r = s^2$ with $s = m/e \in \mathbb{Q}$ where $\gcd(m, e) = 1$. Then $\gcd(m^2, e^2) = 1$ (any nontrivial common factor of m^2 and e^2 would have a prime factor, which would show up in the factorisation of m^2 and thus of m, and also in that of e^2 and thus of e, absurd), so $r = m^2/e^2$ is of the desired form.

5. We have $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

   First of all, $2 = 2/1$ is not square in $\mathbb{Q}$ by the previous question, so $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (we could also have applied (Exercise 1) or (Eisenstein's criterion) to $x^2 - 2 \in \mathbb{Q}[x]$).

   Next, $\sqrt{3}$ is a root of $x^2 - 3$. If this is irreducible over $\mathbb{Q}(\sqrt{2})$, then we have $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, so we conclude by the tower law. However, we canNOT use Eisenstein for this, as Eisenstein only applies over $\mathbb{Q}$! Instead, we proceed by contradiction: If $x^2 - 3$ were reducible over $\mathbb{Q}(\sqrt{2})$, then by Exercise 1 it would have a root in $\mathbb{Q}(\sqrt{2})$. But the roots are $\pm\sqrt{3}$, so either way we would have $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. By the same logic as in question 2, we conclude that $3/2$ would be a square in $\mathbb{Q}$, which is absurd in view of the previous question.

Finally, we observe that $\sqrt{6} = \sqrt{2}\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so that $\mathbb{Q}\sqrt{2}, \sqrt{3}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and therefore

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) : \mathbb{Q}] = 4$$

and not 8. In contrast to the first part of the question, what happened here is that $x^2 - 6$ is actually reducible over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, since its roots $\pm\sqrt{6}$ are in there.

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 $[L : K] \leqslant n!$.

Solution 7

1. Let $S = \alpha_1 + \cdots + \alpha_n \in \overline{K}$. Then S is a symmetric polynomial in the α_k (more specifically, it agrees with σ_1), so actually $S \in K$. It follows that $\alpha_n = S - \alpha_1 - \cdots - \alpha_{n-1}$ lies in $K(\alpha_1, \cdots, \alpha_{n-1})$, so that

   $$K(\alpha_1, \cdots, \alpha_n) = K(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n) = K(\alpha_1, \cdots, \alpha_{n-1}),$$

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

2. Induction on $n = \deg F$.

   For $n = 1$, F has degree 1, so its unique root α_1 lies in K, so $L = K(\alpha_1) = K$; and indeed

   $$[L : K] = [K : K] = 1 \leqslant 1!.$$

   In the general case, let $E = K(\alpha_1)$. Then $F(x) = (x - \alpha_1)G(x)$, where $G(x) \in E[x]$ has degree $n-1$ and roots $\alpha_2, \cdots, \alpha_n$. Therefore, a splitting field of $G(x)$ over E is

   $$E(\alpha_2, \cdots, \alpha_n) = K(\alpha_1)(\alpha_2, \cdots, \alpha_n) = K(\alpha_1, \cdots, \alpha_n) = L,$$

   so by induction hypothesis, $[L : E] \leqslant (\deg G - 1)! = (n-1)!$. Furthermore, $[E : K] = [K(\alpha_1) : K] = \deg m(x)$, where $m(x)$ is the minimal polynomial of α_1 over K. But $F(\alpha_1) = 0$, so $m(x) \mid F(x)$, so $\deg m \leqslant \deg F = n$. By the tower law, we conclude that

   $$[L : K] = [L : E][E : K] \leqslant (n-1)!n = n!,$$

   so the induction is complete.

   Remark: We have equality iff. $F(x)$ is irreducible over K (so $\deg m = n$) and $G(x) = F(x)/(x-\alpha_1)$ is irreducible over $E = K(\alpha_1)$ and $F(x)/(x-\alpha_1)(x-\alpha_2)$ is irreducible over $K(\alpha_1, \alpha_2)$ and... etc., that is to say if $F(x)/(x-\alpha_1)\cdots(x-\alpha_j)$ is irreducible over $K(\alpha_1, \cdots, \alpha_j)$ for all $0 \leqslant j < n$. We will see that this can actually happen, so the bound $[L : K] \leqslant n!$ can be sharp.

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 $\overline{\mathbb{F}_p}$?

Solution 8

1. Since $F'(x) = nx^{n-1} + b = n(x^{n-1} - \beta^{n-1}) = n\prod_{k=1}^{n-1}(x - \zeta^k\beta)$, the roots of $F'(x)$ are the $\zeta^k\beta$ for $0 \leq k \leq n-2$ (or, more elegantly, for k mod $n-1$).
2. We compute that
$$F(\zeta^k\beta) = \zeta^{kn}\beta^n + b\zeta^k\beta + c = \zeta^k\left(-\frac{\beta}{n}\right) + b\zeta^k\beta + c = \left(1 - \frac{1}{n}\right)\beta\zeta^k b + c.$$
3. It follows that
$$\begin{aligned}
\operatorname{Res}(F, F') &= n^n \prod_{k=0}^{n-2} P(\zeta^k\beta) \qquad \text{because the leading coefficient of } F' \text{ is } n \\
&= n^n \prod_{k=0}^{n-2} \left(\left(1 - \frac{1}{n}\right)\beta\zeta^k b + c\right) \\
&= n^n(-1)^{n-1} \prod_{k=0}^{n-2} \left(-c - \zeta^k\left(1 - \frac{1}{n}\right)\beta b\right) \\
&= n^n(-1)^{n-1}\left(\big(-c\big)^{n-1} - \big((1-1/n)\beta b\big)^{n-1}\right) \text{ as } \prod_{k=0}^{n-2}(x - \zeta^k y) = x^{n-1} - y^{n-1} \\
&= n^n c^{n-1} - n^n\beta^{n-1}b^{n-1}(1/n - 1)^{n-1} \\
&= n^n c^{n-1} - n\left(-\frac{b}{n}\right)(1-n)^{n-1}b^{n-1} \\
&= n^n c^{n-1} + (1-n)^{n-1}b^n.
\end{aligned}$$
Since $F(x)$ is monic, we conclude that
$$\operatorname{disc} F = (-1)^{n(n-1)/2}\operatorname{Res}(F, F') = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big).$$
4. Let $F(x) = x^5 - 5x + 6$. Thanks to the formula established in the previous question, we find that $\operatorname{disc} F = (-4)^4(-5)^5 + 5^5 6^4 = 5^5(6^4 - 4^4) = 5^5 \cdot 1040 = 5^5 \cdot 2^4 \cdot 5 \cdot 13 = 2^4 \cdot 5^6 \cdot 13$.

However, the fact that we could also (in theory) have computed this discriminant as a determinant with integer entries shows that

$$\operatorname{disc}(F \bmod p) = (\operatorname{disc} F) \bmod p$$

for all primes p. Therefore, F has multiple roots in $\overline{\mathbb{F}_p}$ iff. $\operatorname{disc} F = 0 \bmod p$, iff. $p \in \{2, 5, 13\}$.