Galois theory — Exercise sheet 1

https://www.maths.tcd.ie/~mascotn/teaching/2021/MAU34101/index.html

Version: October 6, 2021

Email your answers to mascotn@tcd.ie by Wednesday October 6, 4PM.

Exercise 1 *Fewer roots to generate the splitting field (100pts)*

1. Let K be a field such that $\operatorname{char} K \neq 2$, and let $F(x) = ax^2 + bx + c \in K[x]$ with $a \neq 0$. Finally, let $\overline{K}$ be an algebraic closure of K.

   Observe that $F(x) = a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{(2a)^2}\right)$, where $\Delta = b^2 - 4ac$.

   (a) (10pts) Prove that there exists $\delta \in \overline{K}$ such that $\delta^2 = \Delta$.

   (b) (5pts) Express the roots of $F(x)$ in $\overline{K}$ in terms of δ.

   (c) (35pts) Suppose that Δ is not a square in K (in other words, that $\delta \notin K$). Prove that $F(x)$ is irreducible over K, and that $K(\delta)$ is both a stem field and a splitting field of $F(x)$ over K.

   (d) (15pts) Suppose now that $\delta \in K$. Describe a splitting field of $F(x)$ over K.

   (e) (5pts) What breaks down if $\operatorname{char} K = 2$? (The question merely asks you which part(s) of the logic go wrong; you are not required to find a way to fix what goes wrong.)

2. (30pts) Let K be a field, let $F(x) \in K[x]$ have degree $n \in \mathbb{N}$, 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. Prove that $K(\alpha_1, \cdots, \alpha_{n-1})$ is a splitting field of $F(x)$ over K.

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

Solution 1

1. (a) Since $\overline{K}$ is an algebraic closure of K, the polynomial $x^2 - \Delta \in K[x]$ splits completely over, and thus has all roots in, $\overline{K}$.

   (b) The factorisation $F(x) = a\left(\left(x + \frac{b}{2a}\right)^2 - \left(\frac{\delta}{2a}\right)^2\right) = a\left(x + \frac{b+\delta}{2a}\right)\left(x + \frac{b-\delta}{2a}\right)$ over $\overline{K}$ shows that the roots of $F(x)$ in $\overline{K}$ are $\alpha_+ = \frac{-b+\delta}{2a}$ and $\alpha_- = \frac{-b-\delta}{2a}$.

   (c) $F(x)$ has degree 2, so over any field, either it is irreducible, or it splits into two factors of degree 1 and therefore has at least one root. Therefore, if $F(x)$ were reducible over K, then we would have at least one of $\alpha_\pm \in K$. However, this is impossible: for instance, if we had $\alpha_- \in K$, then as $a, b \in K$, we would also have $\delta = -2a\alpha_- + b \in K$, a contradiction with our assumption that $\delta \notin K$. So $F(x)$ must be irreducible over K.

The same calculation also shows that $\delta \in K(\alpha_-)$, so that $K(\delta) \subseteq K(\alpha_-)$; conversely, clearly $\alpha_- = \frac{-b-\delta}{2a} \in K(\delta)$, so $K(\alpha_-) \subseteq K(\delta)$. In conclusion, $K(\delta) = K(\alpha_-)$ is thus a stem field of $F(x)$ over K.

The same logic with α_+ instead of α_- shows that $K(\delta) = K(\alpha_+)$; in particular, both $\alpha_\pm$ lies in $K(\delta)$, so that $K(\alpha_-, \alpha_+) \subseteq K(\delta)$. Conversely, we have $K(\alpha_-, \alpha_+) \supseteq K(\alpha_-) = K(\delta)$, so we conclude that $K(\delta) = K(\alpha_-, \alpha_+)$ is also a splitting field of $F(x)$ over K.

(d) Since $\delta \in K$, we have that both $\alpha_\pm$ lie in K; therefore $K(\alpha_+, \alpha_-) = K$ itself is a splitting field of $F(x)$ over K.

(e) The identity $F(x) = a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{(2a)^2}\right)$ becomes meaningless, since it involves divisions by $2 = 0$.

2. 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.

This was the only mandatory exercise, that you must submit before the deadline. The following 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 exercise.

Exercise 2 *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 2

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 $\mathbb{F}_p$.

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

   $$x^2+x+1 \text{ has no roots in } \mathbb{F}_2 \Longrightarrow \text{irreducible over } \mathbb{F}_2 \Longrightarrow \mathbb{F}_4 \simeq \mathbb{F}_2[x]/(x^2+x+1),$$
   $$x^2+1 \text{ has no roots in } \mathbb{F}_3 \Longrightarrow \text{irreducible over } \mathbb{F}_3 \Longrightarrow \mathbb{F}_9 \simeq \mathbb{F}_3[x]/(x^2+1),$$
   $$x^2+2 \text{ has no roots in } \mathbb{F}_5 \Longrightarrow \text{irreducible over } \mathbb{F}_5 \Longrightarrow \mathbb{F}_{25} \simeq \mathbb{F}_5[x]/(x^2+2).$$

   A polynomial of degree 3 either factor 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 factor 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 s $2+2$. However 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 3 *Two models for $\mathbb{F}_8$*

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

1. Prove that K and L are fields.
2. Prove that K and L are isomorphic.
3. Let $k(x) = x^3+x+1 \in \mathbb{F}_2[x]$, so that $K = \mathbb{F}_2[x]/k(x)$. Establish a natural bijection between { isomorphisms from K to L } and { roots of $k(x)$ in L }.

   Hint: Prove that any morphism from K to L is automatically an $\mathbb{F}_2$-morphism. What does this imply about the image of the class of x in K by such a morphism?
4. Describe explicitly an isomorphism between K and L.

   Hint: Write $L = \mathbb{F}_2[y]/(y^3+y^2+1)$. Which equation does the class of $y+1 \in L$ satisfy? (Remember that $z = -z$ in characteristic 2, since $2z = 0$.)
5. Describe explicitly *all* the isomorphisms between K and L.

   Hint: Frobenius.

Solution 3

1. The polynomial $x^3 + x + 1$ is of degree 3, so if it were reducible over $\mathbb{F}_2$, then it would have a root in $\mathbb{F}_2$. But it does not vanish at 0 nor at 1, so it is irreducible; therefore K is a field. Similarly, $x^3 + x^2 + 1$ is irreducible, so L is a field.

2. $\#K = 2^{[K:\mathbb{F}_2]} = 2^3 = 8$, and similarly $\#L = 8$. Since K and L are two finite fields of the same cardinal, they must be isomorphic.

3. For clarity, let $\alpha \in K$ be the class of x in K, so that $\alpha^3 + \alpha + 1 = 0$.

   Note that since $\mathbb{F}_2 = \{0, 1\}$, any morphism from K to L will automatically be an $\mathbb{F}_2$-morphism, and must therefore take the root α of $k(x) \in F_2[x]$ to a root of $k(x)$ in L. Conversely, given such a root $\gamma \in L$, the evaluation morphism

   $$\begin{array}{ccc} \mathbb{F}_2[x] & \longrightarrow & L \\ f(x) & \longmapsto & f(\gamma) \end{array}$$

   has its kernel which is by definition generated by the minimal polynomial of γ over $\mathbb{F}_2$, which must be $k(x)$ itself since $k(x)$ is irreducible over $\mathbb{F}_2$ and monic; it therefore induces a morphism from $\mathbb{F}_2[x]/k(x) = K$ to L, which is injective and therefore bijective since $\#K = \#L = 8$.

4. The previous question shows that in order to find an isomorphism between K and L, we must find a root γ of $k(x)$ in L. For clarity, write $L = \mathbb{F}_2[y]/(y^3 + y^2 + 1)$, and let $\beta \in L$ be the class of y in L, so tthat $\beta^3 + \beta^2 + 1 = 0$. Following the hint, we check that $\gamma = \beta + 1$ satisfies

   $$\gamma^2 = \beta^2 + 1 \quad \text{(Frobenius in char. 2)},$$

   $$\gamma^3 = \gamma\gamma^2 = (\beta + 1)(\beta^2 + 1) = \beta^3 + \beta^2 + \beta + 1 = \beta = \gamma - 1$$

   whence $0 = \gamma^3 - \gamma + 1 = \gamma^3 + \gamma + 1$ since we are in characteristic 2. So $\gamma = \beta + 1$ is a root of $k(x)$ in L, whence the isomorphism

   $$\begin{array}{rcl} K = \mathbb{F}_2[x]/(x^3 + x + 1) & \longrightarrow & L = \mathbb{F}_2[y]/(y^3 + y + 1) \\ f(\alpha) = f(x) & \longmapsto & f(\gamma) = f(\beta + 1) = f(y + 1). \end{array}$$

5. By question 3., this amounts to finding all the roots of $k(x)$ in L. We already know that there are at most $\deg k(x) = 3$ of them, so there are at most 3 isomorphisms from K to L.

   Oberserve now that since the Frobenius $l \mapsto l^2$ of L is an $\mathbb{F}_2$-automorphism, it will take any root of $k(x) \in \mathbb{F}_2[x]$ in L to another root of $k(x)$ in L. We can use this idea to try to find new roots of $k(x)$ from our old root $\gamma = \beta + 1$. We thus find the roots $\gamma^2 = (\beta+1)^2 = \beta^2 + 1^2 = \beta^2 + 1$, and $(\beta^2 + 1)^2 = \beta^4 + 1^2 = \beta\beta^3 + 1 = \beta(-\beta^2 - 1) + 1 = \beta(\beta^2 + 1) + 1 = \beta^3 + \beta + 1 = -\beta^2 - 1 + \beta + 1 = \beta^2 + \beta$ since $-l = l$ in characteristic 2. Since these roots are all distinct, there cannot be any more, so we stop there (you can check that applying Frobenius to $\beta^2 + \beta$ would bring us back to our original root γ).

   In conclusion, we have found exactly 3 roots of $k(x)$ in L, and thus 3 isomorphisms from K to L, given respectively by $f(\alpha) \mapsto f(\beta+1)$, $f(\alpha) \mapsto f(\beta^2+1)$, and $f(\alpha) \mapsto f(\beta^2 + \beta)$.

Remark. *Let $i, j : K \simeq L$ be two isomorphisms. Then $j \circ i^{-1} : L \simeq L$ is an automorphism of L. Conversely, if $\sigma \in \mathrm{Aut}(L)$ and $i : K \simeq L$ is an isomorphism, then $\sigma \circ i$ is also an isomorphism from K to L. Therefore, we can find all isomorphisms from K to L by post-composing the isomorphism found in the previous question with automorphisms of L. What we did in this question was to take these automorphisms of L to be iterations of the Frobenius. That this was enough to find all the isomorphisms from K to L comes from the fact that the group $\mathrm{Aut}(L)$ is actually generated by the Frobenius, as we shall see later in this module.*

Exercise 4 *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 4

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 $k \bmod n-1$).
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
$$\begin{aligned}
\mathrm{Res}(P, P') &= n^n \prod_{k=0}^{n-2} P(\zeta^k\beta) \qquad \text{because the leading coefficient of } P' \text{ is } n \\
&= n^n \prod_{k=0}^{n-2} \left(\left(1 - \frac{1}{n}\right)\beta\zeta^k b + c\right) \\
&= n^n(-1)^{n-1} \prod_{k=0}^{n-2} \left(-c - \zeta^k\left(1 - \frac{1}{n}\right)\beta b\right) \\
&= n^n(-1)^{n-1}\left(\big(-c\big)^{n-1} - \big((1-1/n)\beta b\big)^{n-1}\right) \text{ as } \prod_{k=0}^{n-2}(x - \zeta^k y) = x^{n-1} - y^{n-1} \\
&= n^n c^{n-1} - n^n\beta^{n-1}b^{n-1}(1/n - 1)^{n-1} \\
&= n^n c^{n-1} - n\left(-\frac{b}{n}\right)(1-n)^{n-1}b^{n-1} \\
&= n^n c^{n-1} + (1-n)^{n-1}b^n.
\end{aligned}$$

Since $F(x)$ is monic, we conclude that

$$\operatorname{disc} P = (-1)^{n(n-1)/2} \operatorname{Res}(P, P') = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big).$$

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. $p \in \{2, 5, 13\}$.