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?

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 $\mathbb{R}$.

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.

Solution 2

We are going to prove that f induces $\bar{f} : R/I \to S/J$ if and only if $f(I) \subseteq J$.

This condition is necessary because if $\bar{f}$ exists, then $\bar{f}(0) = 0$; but every $i \in I$ represents $0 \in R/I$, so we must have $f(i) = 0 \in S/J$, which means $f(i) \in J$.

Conversely, if $f(I) \subseteq J$, then $\bar{f}(r+I) = \bar{f}(r) + \bar{f}(I)$ is well-defined in S/J for all $r \in R$ since $f(I)$ is always 0 in S/J, so the condition is also sufficient.

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).

Solution 3

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 factors 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 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 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 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 $2z = 0$.)

Solution 4

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, $y^3 + y^2 + 1$ 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. Given fields $E \subset F$ and an irreducible polynomial $P \in E[x]$, the E-morphisms from $E[x]/(P)$ to F are in one-to-one correspondence with the roots γ of P in F, the corresponding morphism being

$$\begin{array}{ccc} E[x]/(P) & \longrightarrow & F \\ f(x) & \longmapsto & f(\gamma). \end{array}$$

So, to find a morphism from $K = \mathbb{F}_2[x]/(x^3 + x + 1)$ to L, we need to find a root of $x^3 + x + 1$ in L. Let β be the image of y in L, so that $\beta^3 + \beta^2 + 1 = 0$. Following the hint, we check that $\alpha = \beta + 1$ satisfies

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

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

whence $0 = \alpha^3 - \alpha + 1 = \alpha^3 + \alpha + 1$ since we are in characteristic 2. So $\alpha = \beta + 1$ is a root of $x^3 + x + 1$ in L, whence a morphism

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

This map is a field morphism, so it is injective; it is therefore bijective since the source and the target have the same finite cardinal (alternatively, its inverse is clearly $g(y) \mapsto g(y - 1) = g(y + 1)$).

Remark. *We will see that L has 3 automorphisms. Therefore, there are actually 3 isomorphisms from K to L. They are in 1-to-1 correspondence with the roots of x^3+x+1 in L, so there are 3 such roots: $\beta+1$, β^2+1, and $\beta^2+\beta+1$, whence the 3 isomorphisms $f(x) \mapsto f(\beta+1)$, $f(\beta^2+1)$, $f(\beta^2+\beta+1)$ from K to L.*

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

Solution 5

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

Solution 6

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.