MA3D5 Galois Theory exercises

Marco Streng

These problems are not for handing in. Please try them before the exercise classes.

The following problems belong to the lecture of Tuesday 4 October:

1. Is $\mathbf{Z}/25\mathbf{Z}$ a ring? Is it a field?

Recall that a *subring* of a ring S is a subset $R \subset S$ such that for the $0, 1, +, \times$ of S and for all $a, b \in R$, we have $0, 1, -a, a+b, a \times b \in R$. A *subfield* of a field L is a subring $K \subset L$ that is a field.

2. Let $i \in \mathbf{C}$ be a square root of -1. Consider the subset $K = \{a + bi \in \mathbf{C} : a, b \in \mathbf{Q}\} \subset \mathbf{C}$.
   (a) Prove that K is a subring of $\mathbf{C}$.
   (b) Prove that for any non-zero $a+bi \in K$, we have that $(a+bi)(a-bi) = a^2 + b^2$ is a non-zero element of $\mathbf{Q}$.
   (c) Prove that K is a subfield of $\mathbf{C}$.
   (d) Prove that we have $K = \mathbf{Q}(i)$, i.e., K is the smallest subfield of $\mathbf{C}$ that contains $\mathbf{Q}$ and i.

3. Does there exist a pair of fields K and L, where K is a subfield of L and $\mathrm{char}(K) \neq \mathrm{char}(L)$?

4. What is the characteristic of $\mathbf{F}_5(X)$? What is its prime subfield?

5. Given a field K and polynomials f and g in $K[X]$, there exist unique q, $r \in K[X]$ with $f = qg + r$ and $\deg r < \deg g$ ("division with remainder"). Give q and r for
   (a) $f = X^4 + X + 1$, $g = X^3 - 3 \in \mathbf{Q}[X]$
   (b) $f = X^3 + X + 2$, $g = X - 2 \in \mathbf{Q}[X]$
   (compare r to $f(2)$, can you explain this?)
   (c) $f = X^2 + 3$, $g = X^5 + X + 2 \in \mathbf{F}_5[X]$

See also exercises (1.1) – (1.4) and (2.4) of [Kr],
or exercises 1 – 6 of Chapter 2 of [Re].

The following problems belong to the lecture of Friday 7 October:

6. Prove that every linear polynomial over a field is irreducible.

7. Let $R = \mathbf{Q}[X]/(X^2 - 1)$ and let $\overline{X}$ denote the image of X in the ring R.

   (a) Write the product of $f = \overline{X} + 2$ and $g = 2\overline{X} - 3$ in the form $a\overline{X} + b$ with a, $b \in \mathbf{Q}$.

   (b) Same as (a), but for $f = \overline{X} + 1$ and $g = \overline{X} - 1$.

   (c) Is R a field?

8. Consider the polynomials $f = X^3 + 2X + 2$, $g = X + 1 \in \mathbf{Q}[X]$.

   (a) Find x and $y \in \mathbf{Q}[X]$ with $xf + yg = 1$.

   Let α denote the image of X in $\mathbf{Q}[X]/(f)$.

   (b) Find a multiplicative inverse $(\alpha + 1)^{-1}$ of $(\alpha + 1)$ and write it in the form $h(\alpha)$ with $h \in \mathbf{Q}[X]$ of degree ≤ 4.

   (c) as (b), but for $(\alpha^2 + 1)$ instead of $(\alpha + 1)$.

9. Find the gcd of the following pair of polynomials using Euclid's algorithm: $f = x^4 - 3x^2 + x + 1$ and $g = x^3 - 2x^2 - x + 2 \in \mathbf{Q}[x]$

See also exercises (2.5), (2.7), (2.8), (3.5), (3.10) and (3.11) of [Kr] and exercises 12, 13 of chapter 2 of [Re].

The following problems belong to the lecture of Tuesday 11 October:

10. Find the minimal polynomial of $\alpha + 1$ of exercise 8. What is the degree of $\alpha + 1$ over $\mathbf{Q}$?

11. For the each of the following 9 pairs (K, α), determine whether α is algebraic or transcendental over K. Where appropriate, determine the minimal polynomial and the degree of α over K.

    (a) $\alpha = i \in \mathbf{C}$ and $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}$

    (b) as (a), but with $\alpha = \sqrt{2}$

    (c) $\alpha = T \in \mathbf{Q}(T)$ and $K = \mathbf{Q}$
    Here $\mathbf{Q}(T)$ is the field of rational functions over $\mathbf{Q}$ with variable T.

    (d) as (c), but with $K = \mathbf{Q}(T)$

    (e) as (c), but with

    $$K = \mathbf{Q}(T^2) = \{\frac{a_m T^{2m} + \cdots + a_1 T^2 + a_0}{b_n T^{2n} + \cdots + b_1 T^2 + b_0} : a_i, b_j \in \mathbf{Q}\} \subset \mathbf{Q}(T),$$

    the field of rational functions in T^2.

12. Give a list of all irreducible polynomials in $\mathbf{F}_2[X]$ of degree ≤ 3.

The following problems belong to the lecture of Tuesday 18 October:

13. (a) Let L/K be a field extension and $\alpha, \beta \in L$ algebraic over K. Prove that $\alpha + \beta$ and $\alpha\beta$ are algebraic over K.

    (b) Prove that the set $\overline{\mathbf{Q}} := \{\alpha \in \mathbf{C} : \alpha \text{ is algebraic over } \mathbf{Q}\}$ is a subfield of $\mathbf{C}$.

    (c) Conclude that algebraic extensions can be infinite.

In problems 14 – 16, the results are more interesting than the methods. It is recommended to try to understand what they mean, and to solve only the one that looks most interesting to you.

14. Prove that all ring homomorphisms between fields are injective.

15. Let L, L' be fields of the same characteristic.

    (a) Prove that L and L' have the same prime subfield, call it K.

    (b) Show that any ring homomorphism $L \to L'$ is a K-homomorphism.

16. Let L/K be a field extension and let $\alpha \in L$ be transcendental over K. Fill in the blanks in the proof of existence of a K-homomorphism $\phi : K(X) \to K(\alpha)$ with $\phi(X) = \alpha$.

17. Let M/L and L/K be field extensions.

    (a) Prove that if M/K is algebraic, then so are M/L and L/K.

    (b) Prove the converse, that is, prove that if M/L and L/K are algebraic, then so is M/K.
    Hint: given any $\alpha \in M$ with minimal polynomial $f_\alpha^L = a_0 + a_1 X + \cdots + a_n X^n \in L[X]$, what does the tower law tell us about the extension

    $$K \subset K(a_0) \subset K(a_0, a_1) \subset \cdots \subset K(a_0, \ldots, a_n) \subset K(a_0, \ldots, a_n, \alpha)?$$

18. Find all homomorphisms

    (a) $\mathbf{F}_5[X]/(X^2+2) \to \mathbf{F}_5[X]/(X^2-2)$ (hint: use problem 15)

    (b) $\mathbf{Q}[X]/(X^{100}+2) \to \mathbf{Q}[X]/(X^{1001}+2)$ (hint: what would the degree of the image be?)

19. Show that there exists an *automorphism* ϕ of $L = \mathbf{Q}(\sqrt{3}, \sqrt{5})$ (i.e., an isomorphism $\phi : L \to L$), such that $\phi(\sqrt{3}) = \sqrt{3}$ and $\phi(\sqrt{5}) = -\sqrt{5}$.

20. Prove that every field extension L/K of prime degree is primitive. [Hint: take $\alpha \in L$ with $\alpha \notin K$; what is the degree of $K(\alpha)/K$?]

See also exercises (2.6), (2.9), (3.9), (3.12), (3.14), (3.16) – (3.19) of [Kr] and 2.21, 2.22, 3.2, 3.4, 3.5, 3.7 – 3.13 of [Re].

The following problem belongs to the lecture of Tuesday 25 October:

21. (a) Let G be a group of order 4. Prove that either G is cyclic or $G \cong C_2 \times C_2$.

    (b) What are the subgroups of G for each case in (a)?

    Let $\alpha = \frac{1+i}{\sqrt{2}} = e^{\pi i/4} \in \mathbf{C}$ and $L = \mathbf{Q}(\alpha)$. Recall (from problem 3 of assignment sheet 1):

    - $\alpha^2 = i$,
    - $(1 - \alpha^2)\alpha = \sqrt{2}$,
    - $L = \mathbf{Q}(\sqrt{2}, i)$,
    - the conjugates of α in L are α, α^3, α^5, α^7
    - $\alpha^8 = 1$.

    (c) Describe all elements of $\mathrm{Aut}(L/\mathbf{Q})$ and give a multiplication table.

    (d) Which type of group from (a) is $\mathrm{Aut}(L/\mathbf{Q})$?

    (e) For $M = \mathbf{Q}$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(i)$, $\mathbf{Q}(i\sqrt{2})$, $\mathbf{Q}(\alpha)$, find $\mathrm{Aut}(L/M)$.

    (f) What can you say about L^H for each subgroup H of $\mathrm{Aut}(L/\mathbf{Q})$?

For the lecture of Friday 28 October, see e.g., [Kr] exercise (4.17).
The following problems belong to the lecture of Tuesday 1 November:

22. Prove that every quadratic extension is normal.

23. Which of the following extensions are Galois? Which are normal?

    (a) $\mathbf{Q}(\zeta)/\mathbf{Q}$ where ζ is a root of unity in $\mathbf{C}$,

    (b) $\mathbf{F}_2(T)/\mathbf{F}_2(T^2)$,

    (c) $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$.

The following problem belongs to the lecture of Friday 4 November:

24. Let $\zeta = e^{2\pi i/7}$ be a primitive 7th root of unity and consider the field extension $\mathbf{Q}(\zeta)/\mathbf{Q}$.

    (a) Determine the automorphism group of this extension. Prove that the extension is Galois and that its Galois group G is cyclic.

    (b) Prove that G has 4 subgroups, and give these subgroups. Draw a diagram of inclusions of these subgroups, and indicate the orders of the subgroups.

    (c) Draw the diagram of intermediate extensions and indicate which subfield of $\mathbf{Q}(\zeta)$ corresponds to which subgroup of G.

    (d) Prove that all of the intermediate fields are Galois over $\mathbf{Q}$.

The following problem belongs to the lecture of Tuesday 8 November.

25. Let K be a subfield of $\mathbf{C}$. Describe the splitting field over K of the polynomial $X^3 - a \in K[X]$ in the following situations:

    (a) K contains a primitive third root of unity, and a is a cube in K;

    (b) K does not contain a primitive third root of unity, and a is a cube in K;

    (c) K contains a primitive third root of unity, and a is not a cube in K;

    (d) K does not contain a primitive third root of unity, and a is not a cube in K.

The following problems belong to the lecture of Friday 11 November. See also [Kr] (6.8) – (6.24).

26. (a) Let L/K and M/L be finite extensions. Show that any normal closure of M/K contains a normal closure of M/L.

    (b) Give an example of a tower of finite extensions M/L and L/K such that both M/L and L/K are normal, but M/K is not normal. Hint: see problems 2 and 4 of assignment sheet 2.

    (c) Give an example where the inclusion of (a) is not an equality, i.e., the normal closure of M/K is larger than the normal closure of M/L.

27. Let $K(\alpha)/K$ be a finite primitive extension and $L/K(\alpha)$ a finite extension. Show that L is a normal closure of $K(\alpha)/K$ if and only if it is a splitting field of f_α^K over K.

The following problems belong to the lecture of Tuesday 15 November. See also the problems for Friday 11 November.

28. Which of the field extensions from problem 23 are separable?

29. (a) Show that any field of characteristic 0 is perfect.

    (b) Let K be a field of characteristic $p > 0$. Prove that the map $K \to K : x \mapsto x^p$ is a field homomorphism. It is called the *Frobenius* map of K.

    (c) Show that a field of characteristic $p > 0$ is perfect if and only if its Frobenius map is an automorphism. Hint: recall that inseparable irreducible polynomials f are of the form $f = g(X^p)$. What does a polynomial $h(X)^p$ look like?

The following problem belongs to the lecture of Friday 18 November. See also [Kr] (7.3)

30. Let L/K be a finite extension of degree n and let p be the characteristic of K (so p is prime or 0). Show that if p does not divide n, then L/K is separable.

For the lecture of Tuesday 22 November, see exercises (7.2), (7.4) – (7.7) of [Kr].

The following problems belong to the lectures of Friday 25 November and Tuesday 29 November. There are quite a few, so you may want to choose the one that intrigues you most.

Recall that a finite field extension L/K with $\mathrm{char}(K) = 0$ is constructible if there exists a tower $K = K_0 \subset K_1 \subset \cdots \subset K_n$ with $L \subset K_n$ and $[K_{i+1} : K_i] \in \{1, 2\}$ for all i.

31. Note: in problem 4 of assignment 4, you may use problem 31 only if you include its proof when handing in the assignment.

    (a) Show that a complex number is constructible if and only if its real and imaginary parts are. [Hint: First show that if z is constructible, then so is $\overline{z}$. Then relate z and $\overline{z}$ to the real and imaginary parts of z as in the lecture.]

    (b) Conclude that if we identify the Euclidean plane $\mathbf{R}^2$ with the set of complex numbers $\mathbf{C}$ in the usual way, then an element is constructible as a point if and only if it is constructible as an element of $\mathbf{C}$.

32. Prove that the normal closure of a constructible field extension is constructible. [Hint: see the proof of the analogous result for solvable field extensions.]

33. Let $z \in \mathbf{C}$ be a root of an irreducible polynomial $f \in \mathbf{Q}[X]$ and let $G = \mathrm{Gal}(L/\mathbf{Q})$ be the Galois group of its splitting field. Prove that if z is constructible, then $\#G$ is a power of two. [Hint: use 32.]

34. Prove the converse of 33, i.e., if $\#G$ is a power of two, then z is constructible. [Hint: Let G be a finite p-group. Prove $\#Z(G) \equiv \#G \bmod p$ by considering the conjugation action. Use this and induction to show that G is solvable.] Note: problem 34 is harder than problem 4 of assignment 4, so don't use it (unless you solve it and include a proof when handing in the assignment).

The following problems belong to the lecture of Friday 2 December (but don't need anything from that lecture, just from the one before).

35. Prove that every dihedral group D_n is solvable.

36. Let K be a field of characteristic p and $a \in K$ an element such that the polynomial $f = X^p - X - a$ is irreducible. Let α be a root of f in an extension L/K.

    (a) Prove that $\alpha + m$ is a root a root of f for any $m \in \mathbf{Z}/p\mathbf{Z}$.

    (b) Prove that $K(\alpha)$ is a splitting field of f.

    (c) Conclude that $K(\alpha)/K$ is Galois.

(d) Prove that $\mathrm{Gal}(K(\alpha)/K)$ is cyclic of order p

The following problems belong to the lecture of Tuesday 6 December.

37. Let $f \in K[X]$ be a polynomial of degree n with no repeated roots in its splitting field L/K. Prove that if $\mathrm{Gal}(f) \subset S_n$ is transitive, then f is irreducible.

38. Show that A_3 and S_3 are the only transitive subgroups of S_3.

39. Show that every transitive subgroup of S_4 is a conjugate of one of the following groups: $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$, $C_4 = \langle(1234)\rangle$, $D_4 = \langle(1234), (13)\rangle$, A_4 and S_4.

40. Give all possible Galois groups of *reducible* cubic polynomials with no repeated roots.

41. Let f be an irreducible cubic polynomial over a finite field. Show that its discriminant is a square.

42. Give the Galois group of $x^3 + 2x + 2$ over $\mathbf{Q}$.