Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin
Ollscoil Átha Cliath | The University of Dublin

Faculty of Engineering, Mathematics and Science

School of Mathematics

JS/SS Maths/TP/TJH **Michaelmas Term 2019**

Galois theory

Nicolas Mascot

Instructions to Candidates:

This exam contains **four** exercises. However, you must only attempt **three** of them: exercise 1 (**mandatory**), and **any two** of exercises 2, 3, and 4.
Non-programmable calculators are permitted for this examination.

You may not start this examination until you are instructed to do so by the Invigilator.

Exercise 1 *Bookwork (30 pts)*

1. *(10 pts)* Let K be a field, and $P(x) \in K[x]$ be an irreducible polynomial. Give the definition of the *stem field* and of the *splitting field* of $P(x)$ over K. Give an example of K and $P(x)$ where the stem field and the splitting field are not the same.

2. *(10 pts)* State the Galois correspondence.

3. *(10 pts)* Let K be a field, let $F(x) \in K[x]$, and let G be the Galois group of $F(x)$ over K. Which property must G have for $F(x)$ to be solvable by radicals over K? Explain what this property means in terms of subgroups of G. Give an example of a group G that satisfies this property, and of one that does not (no justification needed).

Solution 1

1. The stem field is the field generated over K by *one* root of $P(x)$, whereas the splitting field is the field generated over K by *all* the roots of $P(x)$. For instance, if $K = \mathbb{Q}$ and $P(x) = x^3 - 2$, then a stem field is $L = \mathbb{Q}(\sqrt[3]{2})$ (the fields obtained by choosing other roots of $P(x)$ are isomorphic to this one), whereas the splitting field is $N = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) = L(\zeta_3)$, where $\zeta_3 = e^{2\pi i/3}$. Since $L \subset \mathbb{R}$ whereas $\zeta_3 \notin \mathbb{R}$, we have $\zeta_3 \notin L$, so $N = L(\zeta_3) \supsetneq L$.

2. Let $K \subset L$ be a finite Galois extension of Galois group $G = \mathrm{Gal}(L/K)$. Then the maps

$$\begin{array}{rcl} \{\text{subgroups of } G\} & \longleftrightarrow & \{\text{intermediate extensions } K \subseteq E \subseteq L\} \\ H & \longmapsto & L^H \\ \mathrm{Gal}(L/E) & \longleftarrow & E \end{array}$$

are bijections and are inverses of each other. Furthermore, the intermediate extension E is Galois over K iff. the corresponding subgroup H is normal in G.

3. *(10 pts)* $F(x)$ is solvable by radicals over K if and only if G is *solvable*, which means that there exists a *composition series*

$$\{\mathrm{Id}\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

with G_{i+1}/G_i *Abelian* for all i. Another equivalent characterisation is that the iterated derived subgroup $D^n(G)$ is reduced to $\{\mathrm{Id}\}$ for n large enough. For example, $\mathbb{Z}/2\mathbb{Z}$ is solvable (since it is Abelian), whereas the symmetric group S_5 is not solvable (since $D(A_5) = A_5$).

Exercise 2 *Nested radicals (35 pts)*

Let $\alpha = \sqrt{3+\sqrt{5}}$ and $\beta = \sqrt{3-\sqrt{5}}$, so that α and β are both roots of $F(x) = (x^2-3)^2-5$. Finally, let $L = \mathbb{Q}(\alpha)$.

1. *(6 pts)* Prove that $[L : \mathbb{Q}] = 4$.

2. *(7 pts)* Prove that L is a Galois extension of $\mathbb{Q}$.

   Hint: Compute $\alpha\beta$.

3. *(6 pts)* Prove that $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

4. *(8 pts)* Sketch a diagram showing all fields E such that $\mathbb{Q} \subseteq E \subseteq L$, and identifying these fields explicitly. Justify your answer.

   Hint: Compute $(\alpha+\beta)^2$.

5. *(8 pts)* Prove that $F(x)$ is reducible mod p for every prime number $p \in \mathbb{N}$.

Solution 2

(This exercise is similar to an example seen in class.)

1. We have $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset L$, and clearly $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. We thus need to prove that $[L : \mathbb{Q}(\sqrt{5})] = 2$, i.e. that $3+\sqrt{5}$ is not a square in $\mathbb{Q}(\sqrt{5})$. And indeed, if it were the case, then there would exist $a, b \in \mathbb{Q}$ such that $3+\sqrt{5} = (a+b\sqrt{5})^2 = a^2+5b^2+2ab\sqrt{5}$, whence $a^2+5b^2 = 3$ and $2ab = 1$ since $(1, \sqrt{5})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{5})$. Replacing b with $1/2a$ yields $a^4 - 3a^2 + 5/4 = 0$, whence $a^2 = \frac{3\pm\sqrt{4}}{2}$ whence $a^2 = 1/2$ or $5/2$, absurd since $a \in \mathbb{Q}$.

2. We find that $\alpha\beta = 2$, whence $\beta = 2/\alpha \in L$. Therefore, the roots $\pm\alpha$, $\pm\beta$ of $F(x)$ all lie in L, so L is the splitting field of $F(x)$ over $\mathbb{Q}$, and is therefore normal over $\mathbb{Q}$. It is also separable over $\mathbb{Q}$ since we are in characteristic 0.

3. The elements $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ are determined by what they do to the generator α. Besides $\sigma(\alpha)$ must be one of the 4 roots of $F(x)$. Since $\# \mathrm{Gal}(L/\mathbb{Q}) = [L : \mathbb{Q}] = 4$ by the previous questions, the 4 elements of $\mathrm{Gal}(L/\mathbb{Q})$ are Id, $\sigma_1 : \alpha \mapsto -\alpha$, $\sigma_2 : \alpha \mapsto \beta = 2/\alpha$, and $\sigma_3 : \alpha \mapsto -\beta = -2/\alpha$. Since all of these are involutions (e.g. $\sigma_3^2(\alpha) = \sigma_3(-2/\alpha) = -2/\sigma_3(\alpha) = \alpha$), we have $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

4. We have seen in class that the subgroup diagram of $\mathrm{Gal}(L/\mathbb{Q})$ is

$$\begin{tikzcd}
& \{\mathrm{Id}\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{\mathrm{Id}, \sigma_1\} \arrow[dr, dash] & \{\mathrm{Id}, \sigma_2\} \arrow[d, dash] & \{\mathrm{Id}, \sigma_3\} \arrow[dl, dash] \\
& \mathrm{Gal}(L/\mathbb{Q}) &
\end{tikzcd}$$

Clearly, the subfield corresponding to $\{\mathrm{Id}\}$ is L, and that corresponding to $\mathrm{Gal}(L/\mathbb{Q})$ is $\mathbb{Q}$. Let us denote the 3 other ones by $E_i = L^{\{\mathrm{Id}, \sigma_i\}}$ ($i = 1, 2, 3$), so that the elements of E_i are the fixed points of σ_i; besides we know that $[E_i : \mathbb{Q}] = [\mathrm{Gal}(L/\mathbb{Q}) : \{\mathrm{Id}, \sigma_i\}] = 2$.

Since $\sigma_1(\alpha) = -\alpha$, $\alpha^2 = 3 + \sqrt{5}$ is fixed by σ_1, so $E_1 = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{5})$.

Since $\sigma_2(\alpha) = \beta$, $\alpha + \beta$ is fixed by σ_2; besides $(\alpha + \beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta = 6 + 4 = 10$, so E_2 contains $\alpha + \beta = \sqrt{10}$. Since $[E_2 : \mathbb{Q}] = 2$, we deduce that $E_2 = \mathbb{Q}(\sqrt{10})$.

Since $\sigma_3(\alpha) = -\beta$, $\alpha - \beta$ is fixed by σ_3; besides $(\alpha - \beta)^2 = \alpha^2 + \beta^2 - 2\alpha\beta = 6 - 4 = 2$, so E_3 contains $\alpha - \beta = \sqrt{2}$. Since $[E_3 : \mathbb{Q}] = 2$, we deduce that $E_3 = \mathbb{Q}(\sqrt{2})$.

In conclusion, the subfield diagram is

$$\begin{array}{ccccc} & & L & & \\ & \diagup & | & \diagdown & \\ \mathbb{Q}(\sqrt{5}) & & \mathbb{Q}(\sqrt{10}) & & \mathbb{Q}(\sqrt{2}) \\ & \diagdown & | & \diagup & \\ & & \mathbb{Q} & & \end{array}$$

5. Two cases: If p divides $\operatorname{disc} f$, then $f \bmod p$ ha a repeated factor and is thus reducible. If now p does not divide $\operatorname{disc} f$, then the factorisation pattern of $f \bmod p$ represents the cycle decomposition of an element of $\operatorname{Gal}(L/\mathbb{Q})$ acting on the roots of f. If this element is Id, then f splits completely mod p. Else, this element is one of the σ_i, which act as product of two disjoint transpositions, so $f \bmod p$ has two irreducible factors of degree 2. Either way, $f \bmod p$ is always reducible (even though f is irreducible over $\mathbb{Z}$!).

Exercise 3 *A polynomial with Galois group A_4 (35 pts)*

Let $F(x) = x^4 - 2x^3 + 2x^2 + 2 \in \mathbb{Q}[x]$. We denote the roots of $F(x)$ in $\mathbb{C}$ by α_1, α_2, α_3, and α_4.

In this exercise, you may use without proof the following facts:

- *The discriminant of f is $\Delta_f = 3136 = 2^6 \cdot 7^2$.*
- *The transitive subgroups of the symmetric group S_4 are*
  - *S_4 itself,*
  - *the alternate group A_4,*
  - *the dihedral group D_8 of symmetries of the square,*
  - *the Klein group $V_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$,*
  - *and the cyclic group $\mathbb{Z}/4\mathbb{Z}$.*

1. *(2 pts)* Show that $F(x)$ is irreducible over $\mathbb{Q}$.
2. *(7 pts)* Show that $F(x)$ factors mod 3 as a linear factor times an irreducible factor of degree 3.
3. *(8 pts)* Show that the Galois group of $F(x)$ is A_4.
4. *(9 pts)* Prove that $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\alpha_1, \alpha_2)$.
5. *(9 pts)* Determine the degrees of the irreducible factors of $F(x)$ over $\mathbb{Q}(\alpha_1)$.

Solution 3

1. This follows from the fact that f is Eisenstein at 2.
2. First of all, f has a root mod 3, namely $x = 1 \bmod 3$. In particular, $F(x)/(x-1) \in \mathbb{F}_3[x]$; we compute that actually $F(x) \equiv (x-1)(x^3 - x^2 + x + 1) \bmod 3$. Besides $g(x) = x^3 - x^2 + x + 1$ has no roots in $\mathbb{F}_3$, so it is irreducible since it has degree 3.

3. Let $G = \mathrm{Gal}_{\mathbb{Q}}(f)$. Then G is a subgroup of S_4. By the first question, G is transitive, so it is one of the groups on the list given at the beginning of the exercise. By the previous question, G contains a 3-cycle; this eliminates all possibilities except S_4 and A_4. Finally, since Δ_f is a square in $\mathbb{Q}$, G is contained in A_4.

4. Let $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and $E = \mathbb{Q}(\alpha_1, \alpha_2)$. We know that L is Galois over $\mathbb{Q}$, with Galois group A_4. The subgroup H corresponding to E is the subgroup of A_4 consisting of permutations that leave both α_1 and α_2 fixed. In S_4, the only such permutations are Id and (34), but $(34) \notin S_4$, so $H = \{\mathrm{Id}\}$. Therefore $E = L$.

5. Let $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ above, and $E' = \mathbb{Q}(\alpha_1)$. Clearly, we have the (possibly incomplete) factorisation $F(x) = (x - \alpha_1)h(x)$ over E', where $h(x) = (x - \alpha_2)(x - \alpha_3)(x - \alpha_4) = F(x)/(x - \alpha_1) \in E'[x]$. The subgroup H' corresponding to E' is the stabiliser of α_1. In particular, it contains the 3-cycle $\sigma = (234)$. Since $\sigma \in H' = \mathrm{Gal}(L/E')$ permutes the roots of $h(x)$ transitively, $h(x)$ is irreducible over E'. We thus have two irreducible factors, one of degree 1 and one of degree 3.

Exercise 4 *Abelian Galois group (35 pts)*

Let K be a field, $P(x) \in K[x]$ irreducible and separable, $L \supset K$ the splitting field of $P(x)$ over K, and $\alpha \in L$ a root of $P(x)$.

1. *(5 pts)* Explain why L is a Galois extension of K.

2. *(30 pts)* We now suppose that the group $\mathrm{Gal}(L/K)$ is Abelian. Prove that $K(\alpha) = L$.

   Hint: What does the fact that $\mathrm{Gal}(L/K)$ *is Abelian imply about its subgroups?*

Solution 4

1. The extension $K \subset L$ is normal since it is a splitting field, and separable since $P(x)$ is separable.

2. Let $H = \mathrm{Gal}\left(L/K(\alpha)\right)$. It is a subgroup of $\mathrm{Gal}(L/K)$, and actually a *normal* subgroup since $\mathrm{Gal}(L/K)$ is Abelian. Therefore, $K(\alpha)$ is Galois over K. In particular, it is normal

over K. Since the irreducible polynomial $P(x) \in K[x]$ has one root in $K(\alpha)$, it actually has all of it roots in $K(\alpha)$; thus $K(\alpha)$ is the splitting field of $P(x)$ over K, i.e. L.