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

Faculty of Science, Technology, Engineering and Mathematics

School of Mathematics

JS/SS Maths/TP/TJH **Semester 2, 2021**

MAU34101 Galois theory

Never **Nowhere** **Ever**

Dr. Nicolas Mascot

Instructions to candidates:

Additional instructions for this examination:

This is a mock exam paper for revision purposes only.

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

Question 1 *Subgroups for appetiser*

Sketch a diagram showing all the subgroups of G when:

1. $G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$,
2. $G = V_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} < S_4$,
3. $G = S_3$,
4. $G = \mathbb{Z}/n\mathbb{Z}$, for n up to 12.

Question 2 *Bookwork*

Let $K \subset L$ be a finite extension, and let $\Omega \supset K$ be algebraically closed. Which inequalities do we always have between $[L : K]$, $\#\operatorname{Aut}_K(L)$, $\#\operatorname{Hom}_K(L, \Omega)$? When are they equalities? State equivalent conditions.

Question 3 *Correspondence in degree 3*

Let K be a field, and $F(x) \in K[x]$ be separable and of degree 3. Denote its 3 roots in its splitting field L by $\alpha_1,\ \alpha_2,\ \alpha_3$.

1. What are the possibilities for $\operatorname{Gal}_K(F)$? How can you tell them apart?
2. For each of the cases found in the previous question, sketch the diagram showing all the fields $K \subset E \subset L$ and identifying these fields. In particular, locate $K(\alpha_1)$, $K(\alpha_2)$, $K(\alpha_3)$, $K(\alpha_1, \alpha_2)$, etc.
3. In which of the cases above is the stem field of F isomorphic to its splitting field? (*Warning: there is a catch in this question.*)

Question 4 *The fundamental theorem of algebra*

The goal of this Question is to use Galois theory to prove by contradiction that $\mathbb{C}$ is algebraically closed.

You may use without proof the following facts:

- If $F(x) \in \mathbb{R}[x]$ is a polynomial *of odd degree*, then $F(x)$ has at least one root in $\mathbb{R}$.
- If $G(x) \in \mathbb{C}[x]$ is a polynomial *of degree* 2, then $G(x)$ has at least one root in $\mathbb{C}$.
- If G is a finite group of cardinal $\#G = 2^a b$ with b odd, then G has at least one subgroup of cardinal 2^a.
- If H is a finite group whose cardinal $\#H = 2^a$ is a power of 2, then for each integer $0 \leqslant n \leqslant a$, H has at least one subgroup of cardinal 2^n.

1. Prove that if $\mathbb{C}$ were not algebraically closed, then there would exist a finite nontrivial extension K of $\mathbb{C}$ (that is to say $K \supsetneq \mathbb{C}$ and $1 < [K : \mathbb{C}] < \infty$).
2. Deduce that there would exist a finite nontrivial extension $\mathbb{C} \subsetneq L$ such that the extension $\mathbb{R} \subsetneq L$ is Galois.
3. Prove that $[L : \mathbb{R}]$ would necessarily be a power of 2.
4. Prove that there would exist an intermediate field $\mathbb{C} \subsetneq F \subseteq L$ such that $[F : \mathbb{C}] = 2$.
5. Derive a contradiction.

Note: the admitted facts at the top of the Question follow respectively from elementary calculus (limits at $\pm\infty$ and then intermediate value theorem), the formula to solve quadratic equations and the fact that every element of $\mathbb{C}$ admits a square root in $\mathbb{C}$, Sylow's theorem, and Sylow's theorem again.

Question 5 *Galois group computations*

Determine the Galois group over $\mathbb{Q}$ of the polynomials below, and say if they are solvable by radicals over $\mathbb{Q}$.

1. $x^3 - x^2 - x - 2$,
2. $x^3 - 3x - 1$,
3. $x^3 - 7$,
4. $x^5 + 21x^2 + 35x + 420$,
5. $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Question 6 *A cosine formula*

Let $c = \cos(2\pi/17)$.

1. Prove that the group $(\mathbb{Z}/17\mathbb{Z})^\times$ is cyclic, and find a generator for it.
2. Prove that c is algebraic over $\mathbb{Q}$.
3. Determine the conjugates of c over $\mathbb{Q}$, and its degree as an algebraic number over $\mathbb{Q}$.
4. Explain how one could in principle use Galois theory (and a calculator / computer) to find an explicit formula for c.

Question 7 *Extensions of finite field are Galois*

Let $p \in \mathbb{N}$ be prime, $n \in \mathbb{N}$, and $q = p^n$.

1. Give two proofs of the fact that the extension $\mathbb{F}_p \subset \mathbb{F}_q$ is Galois: one by viewing $\mathbb{F}_q$ as a splitting field, and the other by considering the order of $\mathrm{Frob} \in \mathrm{Aut}(\mathbb{F}_q)$.
2. What does the Galois correspondence tell us for $\mathbb{F}_p \subset \mathbb{F}_q$?
3. Generalise to an arbitrary extension of finite fields $\mathbb{F}_q \subset \mathbb{F}_{q'}$.