Australian National University

Student Number:

u							

Mathematical Sciences Institute

EXAMINATION: Final examination — June 2022

MATH 3345/6215

Exam Duration: 180 minutes.
Reading Time: 0 minutes.

Materials Permitted In The Exam Venue:

- None.

Materials To Be Supplied To Students:

- None.

Instructions To Students:

- You must justify all your answers, except where stated otherwise.
- Standard notation:
  - If p is a prime number, then $\mathbb{F}_p$ denotes $\mathbb{Z}/p\mathbb{Z}$.
  - ζ_n denotes the complex number $e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$
  - S_n denotes the group of permutations of the set $\{1, \ldots, n\}$.

Q1	Q2	Q3	Q4	Q5	Q6
32	20	15	15	10	10

Total / 102

Question 1 **32 pts**

Give examples of the following, or if no example exists, state that. In either case, briefly justify your answer.

(a) A ring homomorphism $\mathbb{F}_3 \to \mathbb{C}$.

(b) An extension of $\mathbb{Q}(i)$ of degree 123.

(c) An irreducible polynomial of degree 4 over $\mathbb{F}_2$.

(d) A separable extension which is not normal.

(e) A normal extension which is not separable.

(f) An irreducible cubic polynomial over $\mathbb{F}_7$ with Galois group S_3.

(g) An irreducible polynomial of degree 4 in $\mathbb{Q}[x]$ which has a non-constructible real root.

(h) A polynomial $f(x) \in \mathbb{Q}[x]$ with Galois group S_7.

Question 2 **20 pts**

Let E/F denote an extension of degree 2. Let p denote the characteristic of F.

(a) Prove that if $p \neq 2$, then $E = F(\sqrt{a})$ for some element $a \in F$.

(b) Now assume $p = 2$. Is it *sometimes*, *always*, or *never* the case that $E = F(\sqrt{a})$ for some element $a \in F$? (Don't forget to justify your answer.)

(c) Give an example of an extension $E/\mathbb{Q}$ which is not a radical extension but which is contained in an iterated radical extension. (Recall that an extension E/F is *radical* if $E = F(\alpha)$, for some $\alpha \in E$ with the property that there is an integer $n \geq 1$ such that $\alpha^n \in F$ and that E/F is *iterated radical* if is a tower of radical extensions.)

(d) Give an example of an extension $E/\mathbb{Q}$ which is radical but not contained in a Galois extension with abelian Galois group.

Question 3 **15 pts**

(a) Let F be a field. Let $f(x) \in F[x]$ be an irreducible separable polynomial of degree n. Define the Galois group $G_{f(x)}$ in terms of field automorphisms and explain how it can be viewed as a subgroup of S_n.

(b) State the definition of a transitive subgroup of S_n, and prove that $G_{f(x)}$ is indeed a transitive subgroup of S_n.

(c) Give an example of an integer n and a subgroup G of S_n such that $|G|$ is a multiple of n but such that G cannot occur as the Galois group of any irreducible polynomial of degree n over any field F.

Question 4 **15 pts**

Let p be a prime number, and let $n \geq 2$ be an integer. Consider the following three rings with p^n elements: $\mathbb{Z}/p^n\mathbb{Z}$, $(\mathbb{F}_p)^n$, and $\mathbb{F}_{p^n}$. (We restrict to $n \geq 2$, because when $n = 1$, they are all the same.)

(a) Which of the three are isomorphic as rings?

(b) Which of the three are isomorphic as groups?

(c) Which of the three are vector spaces (and over which fields)? Which of these are isomorphic as vector spaces?

Don't forget to justify your answers.

Question 5 **10 pts**

Determine the Galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$. Draw a diagram of the subgroups of G and the corresponding diagram of subfields of $\mathbb{Q}(\zeta_{16})$, making clear which subgroup corresponds to which field. For each of the subfields, find a generator (over $\mathbb{Q}$). Determine which subfields are normal and which are conjugate to which others.

Question 6 **10 pts**

Dirichlet's theorem in number theory states that for any two relatively prime integers a, n, there exist infinitely many prime numbers p such that $p \equiv a \mod n$. Using this theorem (or otherwise), prove that every finite cyclic group occurs as the Galois group of some finite Galois extension E of $\mathbb{Q}$.