## MA-414 (Galois Theory) Tutorial-1

## January 31, 2023

- 1. Show that any field contains either  $\mathbb{Q}$  or  $\mathbb{Z}/(p)$ , for some prime number p, as the smallest subfield. Show that the characteristic of a finite field is a prime number.
- 2. For any integer n, show that  $\sqrt{n}$  is algebraic over  $\mathbb{Q}$ .
- 3. For any prime number p, show that the polynomial  $x^2 p$  has no solution in  $\mathbb{Q}$ .
- 4. For any two prime numbers p and q, show that  $\sqrt{p} + \sqrt{q}$  is algebraic over  $\mathbb{Q}$ .
- 5. If  $\alpha \in \mathbb{C}$  is transcendental over  $\mathbb{Q}$ , show that for any integer  $n \geq 1$ , the number  $\alpha^n$  is transcendental over  $\mathbb{Q}$ .
- 6. Let  $f : [0,1] \to \mathbb{R}$  be a non-constant continuous function. Show that the set  $f([0,1]) := \{f(a) : a \in [0,1]\}$  contains a number transcendental over  $\mathbb{Q}$ .
- 7. Let  $\alpha \in \mathbb{C}$  be a root of the equation  $X^2 + 2 = 0$ . Show that

$$\mathbb{Q}[\alpha] := \{a + \alpha b : a, b \in \mathbb{Q}\}\$$

is a field.

8. Show that the field described in Section 1.2 of the notes is the smallest subfield of K containing all the  $\alpha_i$ .

For the next three questions, let F be a field and  $f(t) \in F[t]$  be a nonzero polynomial. Show the following:

9. For any  $a \in F$ , there is a polynomial  $g(t) \in F[t]$  such that

$$f(t) = g(t)(t-a) + f(a)$$

- 10. For  $a \in F$ , we have f(a) = 0 if and only if t a divides f(t) in F[t].
- 11. The polynomial f(t) can have at most  $\deg(f(t))$  number of roots.

- 12. Let E, K be fields and let  $\phi : E \to K$  be a ring homomorphism. Show that  $\phi$  has to injective. Recall that our rings will always contain 0,1 and  $1 \neq 0$  and a ring homomorphism always sends 1 to 1.
- 13. Let R be an integral domain and let K be its field of fractions. Let F be a field. Show that there is a bijective correspondence between the following two sets: {Injective ring homomorphisms  $\phi : R \to F$ } and {Field homomorphisms  $\psi : K \to F$ }.