MA-414 (Galois Theory)
Tutorial-6

March 30, 2023

Notation: For any prime number $p > 0$ and an integer $n > 0$, we denote by $\mathbb{F}_{p^n}$ the finite field of order p^n.

1. Show that for any integer $n > 0$, there is an irreducible polynomial $f(X) \in \mathbb{F}_p[X]$ of degree n.
2. Let F be a finite field of characteristic $p > 0$. If $\alpha \in F$ be a root of a polynomial $f(X) \in \mathbb{F}_p[X]$, show that α^p is also a root of $f(X)$.
3. Let F be a field such that $F^\times := F \setminus \{0\}$ is a cyclic group. Show that F is a finite field.
4. Let n, r be two positive integers such that r divides n. Then for any prime number $p > 0$, show that $X^{p^r} - X$ divides $X^{p^n} - X$.
5. Find the number of distinct irreducible polynomials of degree 3 over the field $\mathbb{F}_3$.
6. Let F be a finite field. Show that the product of all non-zero elements of F is equal to -1 in F.
7. Show that every element of $\mathbb{F}_p$ has exactly one p^{th} root.
8. Factorize $X^{16} - X$ in $\mathbb{F}_4[X]$ and in $\mathbb{F}_8[X]$.
9. Show that the polynomial $X^{p^n} - X$ factors over $\mathbb{F}_p[X]$ as the product of all monic irreducible polynomials of degree d, where d divides n.
10. Let $\alpha \in \overline{\mathbb{F}_p}$. If $E/\mathbb{F}_p(\alpha)$ is an algebraic field extension, determine if E is separable over $\mathbb{F}_p$ or not.
11. Let F be a field of characteristic $p > 0$. Show that $f(X) = X^p - X - a \in F[X]$ is reducible over F if and only if $f(X)$ has a root in F.
12. Let F be a subfield of $\mathbb{C}$ such that F is not a subfield of $\mathbb{R}$. Show that F is a dense subset of $\mathbb{C}$ in the standard topology.
13. Let F be a finite field. Show that, for each element $\alpha \in F$, there exists $\beta, \gamma \in F$ such that $\alpha = \beta^2 + \gamma^2$.

14. Let E be the unique finite field of order p^n. Show that for every $m \geq 1$ there is a unique extension K_m of E such that $[K_m : E] = m$. Show that $\mathrm{Aut}(K_m/E) = \langle Fr^n \rangle$. (HINT: Imitate what we did in class for $n = 1$)

15. Show that every element of $\mathrm{Aut}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$, except for the identity map of $\bar{\mathbb{F}}_p$, has infinite order.

16. Let F be a field of characteristic $p > 0$. Let $\alpha \in \bar{F}$ and $\alpha \notin F^p$. Show that $X^{p^n} - \alpha \in F[X]$ is irreducible, for all integer $n \geq 1$.

17. Let F be a field. Let $f(X) \in F[X]$ be a monic irreducible polynomial of degree at least 2 such that all of its roots (in an algebraic closure of F) are the same. Show that $char(F) = p > 0$, for some prime number p and $f(X) = X^{p^n} - \alpha$, for some integer $n \geq 1$ and $\alpha \in F$.

18. Let F be a field of characteristic $p > 0$. Let E/F be a finite degree field extension such that $p \nmid [E : F]$. Show that E is separable over F.

19. Let F be a field of characteristic $p > 0$. Show that $\alpha \in \bar{F}$ is separable over F if and only if $F(\alpha) = F(\alpha^{p^n})$, for all integer $n \geq 1$.

20. Let $f(X) \in F[X]$ be an irreducible polynomial of degree $n > 0$. If the characteristic of F does not divide n, show that $f(X)$ has no multiple roots.

21. Let F be a field and let V be an F vector space. Let $V_i \subset V$ be finitely many proper subspaces. If $V = \cup_{i=1}^r V_i$, show that there is a subset $S \subset \{1, 2, \ldots, r\}$ such that

    (a) $V = \cup_{j \in S} V_j$

    (b) For $j \in S$, we have $V_j \not\subset \left(\cup_{l \in S \setminus j} V_l \right)$.

    (We are simply finding a minimal collection whose union is V) So we may assume that $V = \cup_{i=1}^r V_i$ and the V_i satisfy the second property above. Let $v_1 \in V_1$ be such that $v_1 \notin \cup_{i \neq 1} V_i$. Similarly, let $v_2 \in V_2$ be such that $v_2 \notin \cup_{i \neq 2} V_i$. Show that for any i there is at most one $\lambda \in F$ such that $v_1 + \lambda v_2 \in V_i$. If F is infinite, show that V cannot be written as a finite union of proper subspaces.

22. Let F be a field of characteristic $p > 0$. Let $E = F(\sqrt[p]{\alpha}, \sqrt[p]{\beta})$, for some $\alpha, \beta \in F$, be such that $[E : F] = p^2$. Show that

    (a) F is an infinite field,

    (b) $E \neq F(\gamma)$ for any $\gamma \in E$, and

    (c) there are infinitely many intermediate field extensions of E/F. Contrast this with the situation when we have a Galois extension.

23. Let F be a field of characteristic $p > 0$. Let E/F be a finite extension. Let $[E : F]_i = p^n$ be the inseparable degree of E/F. Suppose that there is no exponent p^r, with $r < n$, such that the composite field $E^{p^r} F$ is separable over F. Show that $E = F(\alpha)$, for some $\alpha \in E$.

24. Let F be a field of characteristic $\neq 2$. Let $F^\times := F \setminus \{0\}$. Let E/F be a quadratic field extension (that is, $[E : F] = 2$). Let

$$S(E) = \{a \in F^\times : a = b^2, \text{ for some } b \in E\}.$$

(i) Show that $S(E)$ is a subgroup of $F^\times$ containing ${F^\times}^2$.

(ii) Let E and E' be two quadratic extensions of F. Show that there is an F-isomorphism $\phi : E \to E'$ if and only if $S(E) = S(E')$.

(iii) Show that there is an infinite sequence of quadratic field extensions $E_i/\mathbb{Q}$, $i \in \mathbb{N}$, such that $E_i \not\cong E_j$, for all $i \neq j$ in $\mathbb{N}$. Contrast this with the fact that for a finite field K, and for an integer $m \geqslant 1$ there is only one extension of K of degree m.