Problems on Fields, Galois theory, and Modules

1 Practice problems

These problems are intended for you to work on to help you review the material. Several of the practice problems are longer problems than what you will find on the exam, whereas some are much more basic. Do as many as you can. Bring your questions on incompleted problems to the afternoon sessions, and bring your solutions to completed problems to present also in the afternoon sessions.

1.1

1. Prove that the following statements are equivalent for a quadratic $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$.
   (a) $f(x)$ is irreducible over $\mathbb{Q}$
   (b) $\sqrt{b^2 - 4ac} \notin Q$
   (c) $\mathrm{Gal}(\mathbb{Q}(\sqrt{b^2 - 4ac}/Q)$ has order 2.
2. Compute the Galois group over $\mathbb{Q}$ of $x^4 + x^2 + x + 1$.
3. Determine the irreducible polynomial for $i + \sqrt{2}$ over $\mathbb{Q}$.
4. Let α denote the positive real fourth root of 2. Factor the polynomial $x^4 - 2$ into irreducible factors over each of the following fields: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha, i)$.
5. Let K/F be a finite Galois extension. Prove that the Galois group $\mathrm{Gal}(K/F)$ is a finite group.
6. Let F be a field of characteristic 2, and let K be an extension of F of degree 2.
   (a) Prove that K has the form $F(\alpha)$, where α is the root of an irreducible polynomial over F of the form $x^2 + x + a$, and that the other root of this polynomial is $\alpha + 1$.
   (b) Is it true that there is an automorphism of K sending $\alpha \mapsto \alpha + 1$?
7. Let K/F be a Galois extension whose Galois group is the symmetric group S_3. Is it true that K is the splitting field of an irreducible cubic polynomial over F?

8. Let $\zeta = e^{2\pi i/3} \in \mathbb{C}$ be a cube root of 1. Let $\alpha = \sqrt[3]{a + b\sqrt{2}}$, and let K be the splitting field of the irreducible polynomial for α over $\mathbb{Q}$. Determine the possible Galois groups of K over $\mathbb{Q}(\zeta)$.

9. Determine the degree of a primitive 7th root of unity ζ over $\mathbb{Q}(\omega)$, where ω is a primitive 3rd root of unity.

10. Determine the Galois groups of the polynomials $x^8 - 1,\ x^{12} - 1,\ x^9 - 1$.

11. Prove that $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ is a cyclic group of order r, generated by the Frobenius map ϕ. ($\phi(x) = x^p$.)

12. Let ϕ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Determine the rational canonical form, and the Jordan canonical form (over a field containing all the eigenvalues) for ϕ considered as an $\mathbb{F}_p$-linear transformation of the $\mathbb{F}_p$-vector space $\mathbb{F}_{p^n}$.

2 Sample problems

These questions are intended to be more similar to exam problems, in both lenght and difficulty.

1. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine $[K : \mathbb{Q}]$. Prove that K is a Galois extension of $\mathbb{Q}$ and determine its Galois group.

2. Let p be an odd prime. How many elements of $\mathbb{F}_p$ have square roots in $\mathbb{F}_p$? How many have cube roots in $\mathbb{F}_p$?

3. Let $f \in F[x]$ be a separable polynomial of degree n, and let K be a splitting field for f. Prove that $[K : F]$ divides $n!$.

4. Compute the Galois group over $\mathbb{Q}$ of $4x^4 + 12x + 9$. Compute the Galois group over $\mathbb{Q}$ of $x^3 + 3x + 14$.

5. Determine the degree of the splitting field for the following polynomials over $\mathbb{Q}$. (a) $x^4 - 1$ (b) $x^3 - 2$ (c) $x^4 + 1$

6. Determine all automorphisms of the field $\mathbb{Q}(\sqrt[3]{2})$.

7. Let $K \supset L \supset F$ be fields. Prove or disprove:
   (a) If K/F is Galois, then K/L is Galois.
   (b) If K/F is Galois, then L/F is Galois.
   (c) If L/F and K/L are both Galois, then K/F is Galois.

8. Let $\mathbb{F}$ be a field, and let R be the set of 2×2 matrices of the form

$$\{\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{F}\}.$$

   Show that with the usual matrix operations, R is a commutative ring with identity. For which of the following fields $\mathbb{F}$ is R a field: $\mathbb{F} = \mathbb{Q}, \mathbb{C}, \mathbb{F}_5, \mathbb{F}_7$?

9. Let $F \subset K$ be fields and $a, b \in K$ be algebraic over F. Show $a + b$ is algebraic over F.

10. Let p be a prime, $k, n \in \mathbb{Z}_{>0}$. Show $GL_n(\mathbb{F}_p)$ has an element of order p^k iff $n > p^{k-1}$. (where $GL_n(\mathbb{F}_p)$ is invertible $n \times n$ matrices with entries in $\mathbb{F}_p$.)

11. Let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of submodules of M. Prove that $\cup_{i=1}^{\infty}$ is a submodule of M.

12. Let $R = \mathbb{Z}[x]$ and M be the ideal generated by 2 and x, viewed as an R-module. Show M is not free.

13. Let $V = \mathbb{Q}[x]/(x+1)^2 \oplus \mathbb{Q}[x]/(x-1)(x^2+1)^2 \oplus \mathbb{Q}[x]/(x+1)(x^2-1)$. Determine the invariant factors and elementary divisors for V.

14. Given an R-module M, we write $\operatorname{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}$.

    Prove that if R is an integral domain, then $\operatorname{Tor} M$ is a submodule of M, and $\operatorname{Tor}(M/\operatorname{Tor}(M)) = 0$ (i.e. $M/\operatorname{Tor}(M)$ is torsion-free).

    Give an example of a ring R and module M such that $\operatorname{Tor} M$ is not a submodule.

15. Show that every finite abelian group is a torsion $\mathbb{Z}$-module. Give an example of an infinite abelian group that is a torsion $\mathbb{Z}$-module.

16. Show that $\operatorname{Hom}_R(\oplus A_i, B) \simeq \prod_i \operatorname{Hom}_R(A_i, B)$
    $\operatorname{Hom}_R(A, \oplus B_j) \simeq \oplus_j \operatorname{Hom}_R(A, B_j)$.