Extra Problems

MAT544

Spring 2013

Problem 1. *Let R be a commutative ring with $1 \neq 0$, and A, B, C, D be finite R-modules. Suppose*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \to 0$$

is exact. Prove $|A| \cdot |C| = |B| \cdot |D|$.

Problem 2. *Let R be a commutative ring with $1 \neq 0$ and suppose*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is short exact.

(a) *Suppose the sequence above splits with a function $h : C \to B$. Prove $B = Im(f) \oplus Im(h)$.*

(b) *Suppose M is an R-module and N is a submodule such that M/N is a free R-module with finite basis of size k. Prove $M \cong N \oplus R^k$.*

Problem 3. *Let M is an R-module and N be an R-submodule of M. Prove M is Noetherian if and only if N and M/N are Noetherian.*

Problem 4. *Et R be an integral domain and let F be a field contained in R as a subring. Suppose R is finitely generated as an F-module. Show that R is a field.*

Problem 5. *Let $f : A \to B$ be an R-module homomorphism.*

(a) *Show that f is injective if and only if for every pair of R-module homomorphisms $g, h : D \to A$ such that $f \circ g = f \circ h$, then $g = h$.*

(b) *Show that f is surjective if and only if for every pair of R-module homomorphisms $k, t : B \to C$ such that $k \circ f = t \circ f$, then $k = t$.*

Problem 6. *Let R be a commutative ring with $1 \neq 0$ and let M be a free R-module with finite basis of order k. Show that $M \cong R^k$.*

Problem 7. *Let R be a ring with identity. Prove that $Hom_R(R, R)$ is isomorphic to R.*

Problem 8. *Show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are isomorphic as $\mathbb{Q}$-vector spaces, but not as rings.*

Problem 9. *Let M be an R-module for R a commutative ring. Prove that the scalar multiplication of R on M may be extended to $R[x]$ so that M becomes an $R[x]$-module.*

Problem 10. *Prove that a finite subgroup of the multiplicative group of a field must be cyclic.*

Problem 11. *Let E be an extension field of F and let K and L be intermediate fields of E/F. Let $[K : F] = m$ and $[L : F] = n$ and assume $\gcd(m, n) = 1$. Show that $K \cap L = F$ and $[KL : F] = mn$.*

Problem 12. *Let $\mathbb{Q}$ be the field of rational numbers. Show that the group of automorphisms of $\mathbb{Q}$ is trivial.*

Problem 13. *Show that $[F : \mathbb{Q}] = 2$, then there is a square-free integer m such that $F = \mathbb{Q}(\sqrt{m})$.*

Problem 14. *Let K be a Galois extension of F with $|Gal(K/F)| = 12$. Prove that there exists a subfield E of K containing F with $[E : F] = 3$. Does a sub extension L necessarily exist satisfying $[L : F] = 2$?*

Problem 15. *Suppose $K = F(\alpha)$ is a proper Galois extension of F and assume there exists an element σ of $Gal(K/F)$ satisfying $\sigma(\alpha) = \alpha^{-1}$. Show that $[K : F]$ is even and that $[F(\alpha + \alpha^{-1}) : F] = \frac{1}{2}[K : F]$.*

Problem 16. *Let $p \in \mathbb{Z}_+$ be a prime and let $\mathbb{F}_p$ be the finite field with p elements. Let $a \in \mathbb{F}_p \setminus \{0\}$. Show that $f(x) = x^p - x + a \in \mathbb{F}_p[x]$ is irreducible. Let α be a root of of f. Show that $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is Galois.*

Problem 17. *Let K be an extension of $\mathbb{Q}$ contained in $\mathbb{C}$ such that $K/\mathbb{Q}$ is Galois and $Gal(K/\mathbb{Q})$ is cyclic of order 4. Show that $i \notin K$.*

Problem 18. *A field, F, is called* **algebraically closed** *if every polynomial in $F[x]$ has all its roots in F. Show that every algebraically closed field must be infinite.*

Problem 19. *Let K/F be a finite extension of fields. Show that K/F is Galois if and only if $[K : F] = |Aut_F K|$.*

Problem 20. *Let $p > 0$ be a prime and let K be a field with char$K = p$.*

- *(a) Show that if $\zeta \in K$ is a p^{th} root of unity, then $\zeta = 1$. Deduce that if $m, n > 0$ and $p \nmid n$, then every np^m-th root of unity is an n^{th} root of unity.*
- *(b) If $a \in K$, show that the polynomial $x^p - a \in K[x]$ has either no roots or exactly one root in K.*

Problem 21. *Let $F \subseteq K$ be a finite extension of fields and suppose $f(x) \in F[x]$ be a monic irreducible polynomial. Let $\alpha \in K$ be a root of $f(x)$. If K/F is Galois, show that $f(x)$ has all its roots in K.*

Problem 22. *Let K be a Galois extension of k and let $k \subseteq F \subseteq K$ and $k \subseteq L \subseteq K$.*

(a) *Show that* $Gal(K/LF) = Gal(K/L) \cap Gal(K/F)$.

(b) *Show that* $Gal(K/(L \cap F)) = \langle Gal(K/L), Gal(K/F) \rangle$.

Problem 23. *Let* E *be a finite dimensional Galois extension of a field* F *and let* $G = Gal(E/F)$. *For* $e \in E$ *let* $G(e) = \{\sigma(e) : \sigma \in G\}$. *Let* $e_1, \ldots, e_n$ *be all the distinct elements of* $G(e)$.

(a) *Prove that* $f(x) = (x - e_1)(x - e_2) \cdots (x - e_n)$ *is in* $F[x]$.

(b) *Prove that* $f(x)$ *is irreducible in* $F[x]$.

Problem 24. *Let* K_1 *and* K_2 *be two finite extensions of* F *contained in the field* K *and suppose both are splitting fields over* F. *Show that the compositum* K_1K_2 *is a splitting field over* F.

Problem 25. *Let* $K/E/F$ *be a tower of fields. Prove the following:*

(a) *If* $u \in K$ *is separable over* F, *then* u *is separable over* E.

(b) *If* K *is separable over* F, *then* K *is separable over* E *and* E *is separable over* F.

Problem 26. *Let* F *be a field and* $\overline{F}$ *an algebraic closure of* F. *Assume that* $F \subseteq K \subseteq \overline{F}$, $F \subseteq L \subseteq \overline{F}$, K/F *is a Galois extension of fields, and* L/K *is a Galois extension of fields. Prove that* KL/F *is a Galois extension of fields, where* KL *is the composite field.*

Problem 27. *Suppose* $E/\mathbb{Q}$ *is a Galois extension with Galois group isomorphic to* C_6. *Explain why* E *cannot be the splitting field of a cubic polynomial.*

Problem 28. *Suppose that* K *is the splitting field of some polynomial over* $\mathbb{Q}$ *with* $[K : \mathbb{Q}] = p^2q$, *where* p *and* q *are distinct primes. Show that* K *has subfields* L_1, L_2, *and* L_3 *such that* $[K : L_1] = p$, $[K : L_2] = p^2$, $[K : L_3] = q$.

Problem 29. *Let* F *be a perfect field,* $\overline{F}$ *an algebraic closure of* F *and* $\sigma \in Aut(\overline{F}/F)$. *Let*

$$K = \{\alpha \in \overline{F} : \sigma(\alpha) = \alpha\}.$$

Show that K *is a field and that every finite extension of* K *is cyclic.*

Problem 30. *Show that if* F *is a field with characteristic* 0, *then every algebraic extension of* F *is separable. [Hint: If* $f(x) \in \mathbb{Q}[x]$ *has a multiple root, then* $\gcd(f(x), f'(x)) \neq 1$.*]*

Problem 31. *Let* p *be a prime number, and let* K *be the splitting field of* $f(x) = x^6 - p$ *over* $\mathbb{Q}$. *Determine the Galois group of* K *over* $\mathbb{Q}$ *as well as all of the intermediate fields* E *satisfying* $[E : \mathbb{Q}] = 2$.

Problem 32. *Let* p *be an odd prime,* $d \geq 1$ *and write* $q = p^d$.

(a) *Consider* $\{\pm 1\}$ *as a group under multiplication. Show that there is an unique group homomorphism* $\lambda_q : \mathbb{F}_q^\times \to \{\pm 1\}$ *which is characterized by the requirement that for every* $u \in \mathbb{F}_q^\times$, $\lambda_q(u) = 1$ *if and only if* $u = v^2$ *for some* $v \in \mathbb{F}_q^\times$. *Is* λ_q *always surjective?*

(b) Consider the set of all squares in $\mathbb{F}_q$*,*

$$\Sigma_q = \{u^2 \in \mathbb{F}_q : u \in \mathbb{F}_q\} \subseteq \mathbb{F}_q.$$

Show that the number of elements of Σ_q *is* $(q+1)/2$*. Deduce that if* $t \in \mathbb{F}_q$ *then the set*

$$t - \Sigma_q = \{t - u^2 \in \mathbb{F}_q : u \in \mathbb{F}_q\}$$

has $(q+1)/2$ *elements.*

(c) If $t \in \mathbb{F}_q$*, show that*

$$\left|\Sigma_q \cap (t - \Sigma_q)\right| \geq 1.$$

Deduce that every element of $\mathbb{F}_q$ *is either a square or can be written as the sum of two squares.*

(d) Deduce that the equation $x^2 + y^2 + z^2 = 0$ *has at least one non-trivial solution in* $\mathbb{F}_q$*.*

(e) What can you say about the case $p = 2$*?*

Problem 33. *A field* F *is called perfect if every element of an algebraic closure of* F *is separable over* F*. Let* F *be a field of characteristic* p*. Show that the following are equivalent.*

(a) The field F *is perfect.*

(b) For every $\alpha \in F$ *there exists a* $\beta \in F$ *such that* $\beta^p = \alpha$*.*

(c) The map $a \mapsto a^p$ *is an automorphism of* F*.*

Problem 34. *Let* x *and* y *be independent indeterminates of* $\mathbb{F}_p$*,* $K = \mathbb{F}_p(x, y)$*, and* $F = \mathbb{F}_p(x^p, y^p)$*.*

(a) Show that $[K : F] = p^2$*.*

(b) Show that K *is not a simple extension of* F*.*

Problem 35. *Show that every purely inseparable field extension is normal.*

Problem 36. *Let* K *be an arbitrary separable extension of* F*. Show that if every element of* K *is a root of a polynomial in* $F[x]$ *of degree less than or equal to* n*, then* K *is a simple extension of* F *of degree less than or equal to* n*.*

Problem 37. *Let* α *be a root of the polynomial* $x^6 + 3$*. Show that* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *is Galois and find Gal*$(\mathbb{Q}(\alpha)/\mathbb{Q})$*.*

Problem 38. *Let* $q = p^m$ *for* $p, m \in \mathbb{Z}_+$ *with* p *a prime. Let* $g(x) \in F_p[x]$ *be an irreducible polynomial of degree* d*. Show that* $g(x) \mid x^{p^m} - x$ *if and only if* $d \mid m$*.*

Problem 39. *Let* M *be an* R*-module and let* N *be an* R*-submodule of* M*. Prove that* M *is Noetherian (resp. Artinian) if and only if both* N *and* M/N *are Noetherian (resp. Artinian).*

Problem 40. *Let R be a commutative Noetherian ring with identity. Show that there are only finitely many minimal prime ideals of R.*

Problem 41. *Let R be a Noetherian integral domain. Show that every ideal of R contains a product of prime ideals of R.*

Problem 42. *Let M_i be Noetherian R-modules for $i = 1, \ldots, n$. Show that $\bigoplus_{i=1}^{n} M_i$ is a Noetherian R-module.*

Problem 43. *Let M be a Noetherian R-module, and let $f : M \to M$ be an R-module homomorphism. Show that if f is surjective, then f is an R-module isomorphism.*

Problem 44. *Let R be an integral domain. Show that R is Artinian if and only if R is a field.*

Problem 45. *Let V be a vector space over a field F. A linear transformation $T : V \to V$ is said to be idempotent if $T^2 = T$. Prove that if T is idempotent, then $V = V_0 \oplus V_1$, where $T(v_0) = 0$ for all $v_0 \in V$ and $T(v_1) = v_1$ for all $v_1 \in V_1$.*

Problem 46. *Let $T : V \to W$ be a linear transformation of vector spaces over a field F.*

(a) Show that T is injective if and only if $\{T(v_1), \ldots, T(v_n)\}$ is linearly independent in W whenever $\{v_1, \ldots, v_n\}$ is linearly independent in V.

(b) Show that T is surjective if and only if $\{T(x) : x \in X\}$ is a spanning set for W whenever X is a spanning set for V.

Problem 47. *Let V be a finite dimensional vector space over a field F, and $T : V \to V$ a linear transformation. Prove that there exist subspaces W_1 and W_2 of V which are both stable under T such that T restricted to W_1 is non-singular, T restricted to W_2 is nilpotent, and $V = W_1 \oplus W_2$.*

Problem 48. *Show that the center of $M_n(R)$ is isomorphic to the center of R.*

Problem 49. *Let $M_n(F)$ denote the ring of $n \times n$ matrices over a field F, and let I_n denote the identity matrix.*

(a) Determine (with proof) the number of similarity classes there are in $M_n(\mathbb{Q})$ of matrices satisfying $A^2 = -I_n$. Note, your answer may depend on n.

(b) Repeat part (a) for matrices in $M_n(\mathbb{C})$ satisfying $A^2 = -I_n$.

Problem 50. *Let N be an $n \times n$ matrix with coefficients in the field F. Suppose N is nilpotent, that is, $N^k = 0$ for some positive integer k.*

(a) Prove that N is similar to a block diagonal matrix whose blocks are matrices with 1's on the first superdiagonal, and 0's elsewhere.

(b) Prove that if N is an $n \times n$ nilpotent matrix, then $N^n = 0$. (You should not quote the Cayley-Hamilton Theorem).

Problem 51. *Let A be an $n \times n$ complex matrix with characteristic polynomial $f(x) = x^n - nx + 1$.*

(a) Prove that if $n > 2$ then A is diagonalizable over the complex numbers.

(b) Is the assertion in part (a) true if $n = 2$? Either prove it or give a counterexample.

Problem 52. *Let $A \in M_n(\mathbb{C})$. Prove that A is not invertible if and only if 0 is an eigenvalue of A.*

Problem 53. *Let A be an $n \times n$ matrix such that $A^2 = I_n$ and $A \neq I_n$. Show that -1 is an eigenvalue of A.*