Math146 - Review for midterm 2

George McNinch

2025-03-31

I. The exam will cover what is (currently) in sections 8 - 12 of the course lecture notes, namely:

   fields extensions, (constructible numbers), splitting fields, finite fields

   I don't plan on emphasizing §10 on constructible numbers (e.g. since there was no homework on that topic).

   Throughout the discussion below, F denotes a field unless otherwise indicated.

II. You should be able to give careful statements answering the following questions about definitions:

   a. If $F \subset E$ is a field extension, when is an element $\alpha \in E$ *algebraic* F? when is it *transcendental* over F? What is the *minimal polynomial* of α over F? What is the *degree* of α over F? What is meant by the *primitive extension* $F(\alpha)$ of F?

   b. If $F \subset E$ is a field extension and if $\alpha_1, \cdots, \alpha_n \in E$, what is the field extension $F(\alpha_1, \cdots, \alpha_n)$ of F?

   c. What is meant by a *finite extension* $F \subset E$? What is meant by the degree $[E : F]$?

   d. What is meant by an *algebraic extension* $F \subset E$?

   e. If $f \in F[T]$ is a polynomial, what is does it mean to say that f *splits* over an extension field E of F? What is meant by a *splitting field* of f over F?

   f. What is the *characteristic* of F? What is the *prime subfield* of F?

III. You should know the statements of the following:

   a. the result describing an isomorphism between a primitive extension $F(\alpha)$ with a quotient of the polynomial ring $F[T]$ (when α is algebraic) or with the field of fractions of a polynomial ring $F[x]$ (when α is transcendental).

   b. A description of a *basis* for the primitive extension $F(\alpha)$ as an F-vector space, when α is algebraic over F.

   c. If $F \subset E$ and $E \subset K$ are finite extensions, the result relating $[K : F]$, $[K : E]$ and $[E : F]$, and the the result describing an F-basis for K using an E-basis for K and an F-basis for E.

   d. If $F \subset E$ is a field extension, then the elements of E which are algebraic over F form a subfield.

   e. If $u \in \mathbf{R}$ is *constructible* then $[\mathbf{Q}(u) : \mathbf{Q}] = 2^n$ for some $n \in \mathbf{Z}_{\geq 0}$.

   f. The results which guarantee the existence and uniqueness of splitting fields.

g. An upper bound for the degree $[E : F]$ if E is a splitting field for the polynomial $f \in F[T]$.

h. Finite fields: what are their possible orders? How many fields of a give order are there, up to isomorphism? Describe all subfields of a finite field. Describe a finite field as a splitting field over $\mathbf{F}_p$ of a suitable polynomial.

IV. You should be able to write careful solutions to problems similar to the following:

1. Prove: If $F \subset E$ is a finite extension of fields, then E is algebraic over F.
2. If $F \subset E$ is a field extension and if $\alpha_1, \cdots, \alpha_n \in E$ are algebraic over F show that $[F(\alpha_1, \cdots, \alpha_n) : F] < \infty$.
3. Give an example of an irreducible polynomial $g \in F[T]$ and an extension field $F \subset E$ for which f has a root in E but f does not split over E.
4. Let $F \subset E$ be a field extension and let $f, g \in F[T]$. Suppose that there is some $h \in E[T]$ for which $\deg h > 0$, $h \mid f$ and $h \mid g$. Prove that there is some $k \in F[T]$ with $\deg k > 0$, $k \mid f$ and $k \mid g$.
5. Find the minimal polynomial over $\mathbf{Q}$ of $\alpha = \exp(2\pi i/7) \in \mathbf{C}$, and find the degree $[\mathbf{Q}(\alpha) : \mathbf{Q}]$.
6. Let F be a field and let α, β be elements in some extension field of F for which $n = \deg(\alpha)$ and $m = \deg(\beta)$. If $\gcd(n, m) = 1$ show that β also has degree m over $F(\alpha)$.
7. Let $p, q \in F[T]$ be irreducible polynomials with $\deg p = 3$ and $\deg q = 4$. If E is a splitting field for $f = p \cdot q$ over F, prove that $[E : F] \geq 12$.
8. Let $g = T^3 + \dfrac{3}{2} \cdot T + 3 \in \mathbf{Q}[T]$.
   a. Show that g is irreducible.
   b. Let α be a root of g in some extension of $\mathbf{Q}$ and let $E = \mathbf{Q}(\alpha)$. Then $\mathscr{B} = \{1, \alpha, \alpha^2\}$ is an $\mathbf{Q}$-basis for E (why?). Consider the linear transformation $\lambda_\alpha : E \to E$ given by the rule $\lambda_\alpha(x) = \alpha \cdot x$ for $x \in E$. Find the matrix $M_\alpha = [\lambda_\alpha]_{\mathscr{B}}$ of λ_α in the basis $\mathscr{B}$.

      In more detail: write e_0, e_1, e_2 for the standard basis of $\mathbf{Q}^3$ and consider the $\mathbf{Q}$-linear isomorphism $\Phi : \mathbf{Q}^3 \to E$ given by $\Phi(e_i) = \alpha^i$. Find the 3×3 matrix $M = M_\alpha$ for which $\Phi(M \cdot e_i) = \alpha \cdot \alpha^i = \alpha^{i+1}$, being careful to note that α^3 *not* part of the basis $\mathscr{B}$ and so must be re-written.

   c. More generally for $y \in E$ write λ_y for the linear transformation $\lambda_y(x) = y \cdot x$ for $x \in E$. Find the matrix $[\lambda_{\alpha^2}]_{\mathscr{B}}$ and the matrix $[\lambda_{1+\alpha^2}]_{\mathscr{B}}$
9. Consider the field of fractions $\mathbf{C}(X)$ of the polynomial ring $\mathbf{C}[X]$.
   For $a \in \mathbf{C}$, consider the polynomial $q_a = T^2 - (X - a) \in \mathbf{C}(X)[T]$.
   a. Show that q_a is irreducible for each a.
   b. Let $a, b \in \mathbf{C}$ and suppose that $\sqrt{X - a}$ denotes a root of q_a in some extension field. If $a \neq b$, prove that q_b remains irreducible in $\mathbf{C}(X, \sqrt{X - a})[T] = \mathbf{C}(X)(\sqrt{X - a})[T]$.
10. Let $\alpha \in \mathbf{F}_{16}^\times$ be an element of (multiplicative) order 15.
    a. Show that $\mathbf{F}_{16} = \mathbf{F}_2(\alpha)$ and $\mathbf{F}_{16} = \mathbf{F}_2(\alpha^3)$.
    b. For which $i \in \mathbf{Z}$ is it true that $\mathbf{F}_4 = \mathbf{F}_2(\alpha^i)$?

11. Show that if $a, b, c \in \mathbf{Q}$ are pairwise distinct rational numbers, then the elements $\dfrac{1}{X-a}, \dfrac{1}{X-b}, \dfrac{1}{X-c}$ are $\mathbf{Q}$-linearly independent in the field of fractions $\mathbf{Q}(X)$ of $\mathbf{Q}[X]$.

12. Let p be a prime number with $p \neq 2$. Show that there are exactly $(p-1)/2$ non-zero squares in $\mathbf{F}_p$.

    More precisely, show that the set $\{x^2 \mid x \in \mathbf{F}_p^\times\}$ has exactly $\dfrac{p-1}{2}$ elements.

13. Let p be a prime number and let $\mathscr{F} : \mathbf{F}_p \to \mathbf{F}_p$ be the mapping $\mathscr{F}(x) = x^p$. We showed in class that the mapping $\mathscr{F}$ is a ring homomorphism. Using this fact, show that $\mathscr{F}$ is an *automorphism* - i.e. that $\mathscr{F}$ is *bijective*.