Math146 - Review for midterm 2

George McNinch

2025-03-31

1. Prove: If $F \subset E$ is a finite extension of fields, then E is algebraic over F.

Solution: Let $\alpha \in E$; we must show that α is algebraic over F. Since the assumption means that E is finite dimensional as an F-vector space, the (infinite) set $\{\alpha^m \mid m \in \mathbf{Z}_{\geq 0}\}$ is not linearly independent over F. Thus there is some N and elements $a_i \in F$ for $0 \leq i \leq N$ for which

$$0 = \sum_{i=0}^{N} a_i \alpha^i.$$

But then α is a root of the polynomial

$$f(T) = \sum_{i=0}^{N} a_i T^i \in F[T]$$

so indeed α is algebraic over F. Since α was arbitrary, conclude that 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

$$[F(\alpha_1, \cdots, \alpha_n) : F] < \infty.$$

Solution: Proceed by induction on $n \geq 1$. When $n = 1$, the element α_1 is algebraic over F and so $[F(\alpha_1) : F]$ is equal to the degree of the *minimal polynomial* of α_1 over F; in particular, this degree is finite.

Now suppose that $n > 1$ and the result is known for any field F and any collection of $n-1$ elements algebraic over F. We are given $\alpha_1, \cdots, \alpha_n$ algebraic over F.

We know by the induction hypothesis that $[F(\alpha_1, \cdots, \alpha_{n-1}) : F]$ is finite.

Moreover, since degree is multiplicative for iterated extensions, we know

$$[F(\alpha_1, \cdots, \alpha_n) : F] = [F(\alpha_1, \cdots, \alpha_n) : F(\alpha_1, \cdots, \alpha_{n-1})] \cdot [F(\alpha_1, \cdots, \alpha_{n-1}) : F]$$

So to prove the finiteness of the indicated extension, it suffices to argue that $F(\alpha_1, \cdots, \alpha_n)$ is finite over $F(\alpha_1, \cdots, \alpha_{n-1})$. But

$$F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n)$$

so this follows from the observation that α_n is algebraic over $F(\alpha_1, \cdots, \alpha_{n-1})$.

(indeed, the minimal polynomial f of α_n over F may be viewed as a polynomial in $F(\alpha_1, \cdots, \alpha_{n-1})[T]$).

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.

Solution: Here are two examples:

i. Let $F = \mathbf{Q}$, $g = T^3 - 2$ and let α a root of g in some extension field. Then $\mathbf{Q}(\alpha)$ is not a splitting field for g.

   Indeed, denoting by ω a root of $T^2 + T + 1 = \dfrac{T^3 - 1}{T - 1}$ we know that

$$g = (T - \alpha)(T - \omega\alpha)(T - \omega^2\alpha)$$

   in $\mathbf{Q}(\alpha, \omega)$, so that $\mathbf{Q}(\alpha, \omega)$ is a splitting field for g.

   Now, we know that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$ since g is irreducible by Eisenstein. We also know that $[\mathbf{Q}(\omega) : \mathbf{Q}] = 2$ since $T^2 + T + 1$ is irreducible over $\mathbf{Q}$ (by an argument in class which used Eisenstein). Since $\gcd(3, 2) = 1$ we know that $[\mathbf{Q}(\alpha, \omega) : \mathbf{Q}] = 6$ and in particular $\mathbf{Q}(\alpha, \omega) \neq \mathbf{Q}(\alpha)$, so $\mathbf{Q}(\alpha)$ is not a splitting field for g.

ii Let $F = \mathbf{Q}(X)$, $g = T^3 - X$ and let α a root of g in some extension field. Then $\mathbf{Q}(X, \alpha)$ is not a splitting field for g.

   The argument is essentially the same as in i. – a splitting field for g is $\mathbf{Q}(X, \alpha, \omega)$ where again ω is a root of $T^2 + T + 1$, since

$$g = (T - \alpha)(T - \omega\alpha)(T - \omega^2\alpha)$$

   Changing the argument above mutatis mutandum shows that $\mathbf{Q}(X, \alpha) \neq \mathbf{Q}(X, \alpha, \omega)$ so that $\mathbf{Q}(X, \alpha)$ is not a splitting field for g.

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 $k \mid g$.

Solution: Let α be a root of h in some extension field of E and note that α is a root of f and of g. In particular, α is algebraic over F; let's write h for the minimal polynomial of α over F and note that $\deg h \geq 1$.

Now $f(\alpha) = 0$ implies that $h \mid f$ and $g(\alpha) = 0$ implies that $h \mid g$. Thus $k = h$ works as required.

5. Find the minimal polynomial over $\mathbf{Q}$ of $\alpha = \exp(2\pi i/7) \in \mathbf{C}$, and find the degree $[\mathbf{Q}(\alpha) : \mathbf{Q}]$.

Solution: We know that $\alpha = \exp(2\pi i/7 \in \mathbf{C}$ is a root of the polynomial $T^7 - 1$, and since

$\alpha \neq 1$ in fact α is a root of

$$f = \frac{T^7 - 1}{T - 1} = T^6 + T^5 + T^4 + T^3 + T^2 + T + 1 \in \mathbf{Q}[T].$$

Now, we have seen that - since 7 is prime - the polynomial f is *irreducible*. It follows that f is the minimal polynomial of α, and we deduce that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 6$.

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 $F(\alpha)$.

Solution: Let us observe that $n = [F(\alpha) : F]$ and $m = [F(\beta) : F]$. Moreover.

$$(\clubsuit) \quad [F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = n \cdot [F(\alpha, \beta) : F(\alpha)]$$

so that $n \mid [F(\alpha, \beta) : F]$. Similarly, $m \mid [F(\alpha, \beta) : F]$.

Since $\gcd(n, m) = 1$ and since $m \mid [F(\alpha, \beta) : F] = n \cdot [F(\alpha, \beta) : F(\alpha)$ it follows that

$$m \mid [F(\alpha, \beta) : F(\alpha)].$$

On the other hand, we know that $[F(\alpha, \beta) : F(\alpha)] \leq m$ since the minimal polynomial of β over $F(\alpha)$ must divide h_β in the polynomial ring $F(\alpha)[T]$.

Thus we conclude that $[F(\alpha, \beta) : F(\alpha)] = m$; since $F(\alpha, \beta) = F(\alpha)(\beta)$ this shows that the degree of β over $F(\alpha)$ is indeed m as required.

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 $[E : F] \geq 12$.

Solution: Let α, β be roots of p resp. q in some extension field of F. The previous problem shows that q remains irreducible over $F(\alpha)$, so that

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)] \cdot [F(\alpha) : F] = 4 \cdot 3 = 12.$$

Now, there is a splitting field of $f = pq$ containing $F(\alpha, \beta)$, so the degree over F of any splitting field of f is a multiple of 12, as required.

8. Let $g = T^3 + \frac{3}{2} \cdot T + 3 \in \mathbf{Q}[T]$.

   a. Show that g is irreducible.

   Solution: This follows from Eisenstein's criterion. Indeed, it suffices to argue that $2T^3 + 3T + 6 \in \mathbf{Z}[T]$ is irreducible in $\mathbf{Q}[T]$. But this follows from Eisenstein since the prime 3 does not divide the leading coefficient, 3 divides all the remaining coefficients, and 9 does not divide the constant term 6.

   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.

Solution: Note that $\lambda_\alpha(1) = \alpha$, $\lambda_\alpha(\alpha) = \alpha^2$ and $\lambda_\alpha(\alpha^2) = \alpha^3 = -3 + \dfrac{-3}{2}\alpha$. This shows that

$$M = \begin{pmatrix} 0 & 0 & -3 \\ 1 & 0 & -3/2 \\ 0 & 1 & 0 \end{pmatrix}$$

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 $[\lambda_{1+\alpha^2}]_{\mathscr{B}}$

Solution: For any element $y = s + t\alpha + u\alpha^2 \in E$ the matrix $M_y = [\lambda_y]_{\mathscr{B}}$ is given by $sI_3 + tM_\alpha + uM_\alpha^2$

In particular, $M_{\alpha^2} = M^2 = \begin{pmatrix} 0 & -3 & 0 \\ 0 & -3/2 & -3 \\ 1 & 0 & -3/2 \end{pmatrix}$

and $M_{1+\alpha^2} = I_3 + M_{\alpha^2} = \begin{pmatrix} 1 & -3 & 0 \\ 0 & -1/2 & -3 \\ 1 & 0 & -1/2 \end{pmatrix}$

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.

Solution: The irreducibility of q_a follows from Eisenstein. Indeed, $X - a$ is irreducible in $Q[X]$, $X - a$ does not divide the leading coefficient of $q_a = q_a(T)$, $X - a$ divides all remaining coefficients of q_a, and $(X - a)^2$ does not divide the constant term of q_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 $\mathbf{C}(X, \sqrt{X - a})[T] = \mathbf{C}(X)(\sqrt{X - a})[T]$.

Solution: Since q_b has degree 2, to see that q_b remains irreducible in $\mathbf{C}(X, \sqrt{X - a})[T] = \mathbf{C}(X)(\sqrt{X - a})[T]$ it is enough to argue that q_b has no root in $\mathbf{C}(X)(\sqrt{X - a})$.
Let us suppose that $z \in \mathbf{C}(X)(\sqrt{X - a})$ were such a root. Since $\sqrt{X - a}$ has degree 2 over $\mathbf{C}(X)$, we may write z in the form $z = f + g\sqrt{X - a}$ for $f, g \in \mathbf{C}(X)$.
Since z is a root of q_b, we know that $z^2 = X - b$.
But

$$z^2 = f^2 + (X - a)g^2 + 2fg\sqrt{X - a}$$

so the equality $z^2 = X - b$ in $\mathbf{C}(X)(\sqrt{X - a})$ show that $f^2 + (X - a)g^2 = X - b$ and $2fg = 0$.

Since $2fg = 0$, either $f = 0$ or $g = 0$.
If $g = 0$ then we see that $f^2 = X - b$ which is a contradiction since we know by (a) that q_a is irreducible over $\mathbf{C}(X)$.
If $f = 0$ then we see that $(X-a)g^2 = X - b$ which is again a contradiction. Indeed, writing $g = \dfrac{h}{k}$ for $h, k \in \mathbf{C}[X]$ we see that

$$(X-a)h^2 = (X-b)k^2$$

which contradicts unique factorization in the polynomial ring $C[X]$. More precisely, in the LHS, the irreducible polynomial $(X-a)$ appears with odd multiplicity, while since $a \neq b$, $X - a$ appears with even multiplicity on the RHS.

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 $\mathbf{F}_{16} = \mathbf{F}_2(\alpha^3)$.

    Solution: Since $16 = 2^4$, recall that the only subfields of $\mathbf{F}_{16}$ correspond to divisors of 4; thus $\mathbf{F}_2$ and $\mathbf{F}_4$ are the only proper subfields.
    Since α has order 15, and since neither $\mathbf{F}_2^\times$ nor $\mathbf{F}_4^\times$ contain an element of order 15, it follows that $\mathbf{F}_2(\alpha) = \mathbf{F}_{16}$.
    Similarly, since α^3 has multiplicative order 5, and since neither $\mathbf{F}_2^\times$ nor $\mathbf{F}_4^\times$ contain an element of order 5, it again follows that $\mathbf{F}_2(\alpha^3) = \mathbf{F}_{16}$.

    b. For which $i \in \mathbf{Z}$ is it true that $\mathbf{F}_4 = \mathbf{F}_2(\alpha^i)$?

    Solution: Note that $\mathbf{F}_4^\times$ is a cyclic group of order 3. So α^i is contained in $\mathbf{F}_4$ if and only if $o(\alpha^i)$ divides 3, and α^i generates $\mathbf{F}_4$ if and only if $o(\alpha^i) = 3$.
    Thus $\mathbf{F}_4 = \mathbf{F}_2(\alpha^i)$ if and only if either $i \equiv 5 \pmod{15}$ or $i \equiv 10 \pmod{15}$.

11. Show that if $a, b, c \in \mathbf{Q}$ are pairwise distinct rational numbers, then the elements

$$\frac{1}{X-a}, \frac{1}{X-b}, \frac{1}{X-c}$$

are $\mathbf{Q}$-linearly independent in the field of fractions $\mathbf{Q}(X)$ of $\mathbf{Q}[X]$.

Solution: Let $s, t, u \in \mathbf{Q}$ and suppose that

$$\begin{aligned} 0 &= \frac{s}{X-a} + \frac{t}{X-b} + \frac{u}{X-c} \\ &= \frac{s(X-b)(X-c) + t(X-a)(X-c) + u(X-a)(X-b)}{(X-a)(X-b)(X-c)}. \end{aligned}$$

Thus the polynomial $F = s(X-b)(X-c) + t(X-a)(X-c) + u(X-a)(X-b) \in \mathbf{Q}[X]$ is 0. But note that $0 = F(a) = s(a-b)(a-c)$ and hence $s = 0$ since $a \neq b$ and $a \neq c$.
Similarly, $0 = F(b) = t(b-a)(b-c) \implies t = 0$ and $0 = F(c) = u(c-a)(c-b) \implies u = 0$.
Thus we conclude that $s = t = u = 0$ which proves the required linear independence.

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.

    Solution: Consider the group homomorphism $f : \mathbf{F}_p^\times \to \mathbf{F}_p^\times$ given by the rule $f(x) = x^2$.

    The kernel K of this homomorphism consists in the roots of the polynomial $T^2 - 1$. Since $p \neq 2$ there are exactly two such roots: $K = \{\pm 1\} = \{1, p-1\}$. The image of f is precisely the set of squares in $\mathbf{F}_p^\times$.

    According to the first isomorphism theorem, the image of f is isomorphic to the quotient group $\mathbf{F}_p^\times / K$, which has order $|F_p^\times|/|K| = (p-1)/2$ as required.

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.*

    Solution:

    > *The result stated here actually holds for any finite field K, and that is how I should have stated the problem. Namely, we showed in class that $\mathscr{F} : K \to K$ is a ring homomorphism. Using this fact, we can show that $\mathscr{F}$ is an automorphism. This is what I'll prove below.*

    A ring homomorphism $K \to K$ is an automorphism (i.e. is invertible) precisely when it is bijective as a function – i.e. when it is both injective and surjective.

    Since K is a finite set, the function $\mathscr{F} : K \to K$ is bijective if and only if it is injective. Thus, it is enough to argue that $\mathscr{F}$ is injective.

    Let I denote the kernel of $\mathscr{F}$. Then \) is an ideal of the ring K. But K is a field, and so the only ideals of K are $\{0\}$ and K. Since $\mathscr{F}(1) = 1^p = 1 \neq 0$, $1 \notin I$ so that $I \neq \{K\}$. Thus $I = 0$ which implies that $\mathscr{F}$ is injective, as required.