Math146 - Review for the final exam - solutions

George McNinch

2025-05-10

III. You should know the following statements and examples

- a condition for the roots of a polynomial in a splitting field to be distinct

---

Solution: A polynomial $f \in K[T]$ has distinct roots in a splitting field provided that $\gcd(f, f') = 1$ where f' is the formal derivative of f.

- an example of an irreducible polynomial $q \in F[T]$ of degree > 1 such that q has exactly one root in a splitting field E of q over F.

Solution: Let $K = \mathbf{F}_p(X)$ be the field of rational functions over a finite field of prime order p, and consider the polynomial $g = T^p - X \in K[T]$. If L is a splitting field for g over K, let $\alpha \in L$ be a root of g. Then $g(\alpha) = 0 \implies \alpha^p - X = 0 \implies X = \alpha^p$. Then we have the identity

$$g = T^p - X = T^p - \alpha^p = (T - \alpha)^p$$

in $L[T]$ which shows that α is the only root of g in L.

- an example of a non-abelian Galois group

Solution: Let $f = T^3 - 2 \in \mathbf{Q}[T]$. A splitting field over $\mathbf{Q}$ is $K = \mathbf{Q}(\alpha, \omega$ where α is a root of f and where ω is a root of $g = T^2 + T + 1$.
Since f and g are irreducible over $\mathbf{Q}$ of relatively prime degree, we know that $[K : \mathbf{Q}] = 6$. In particular, K is a normal separable extension of $\mathbf{Q}(\omega)$ of degree 3, hence $\mathrm{Gal}(K/\mathbf{Q}(\omega))$ has order 3. In fact, $\mathrm{Gal}(K/\mathbf{Q}(\omega))$ contains an element σ for which $\sigma(\alpha) = \omega\alpha$.
We also know that K is a normal separable extension of $\mathbf{Q}(\alpha)$ of degree 2 hence $\mathrm{Gal}(K/\mathbf{Q}(\omega))$ is 2. In fact, $\mathrm{Gal}(K/\mathbf{Q}(\omega))$ contains an element τ for which $\tau(\omega) = \omega^2$.
Now it is easy to check that $\tau\sigma\tau = \sigma^3$ and in particular $\mathrm{Gal}(K/\mathbf{Q})$ is not abelian.

- a description of the Galois group $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ of the finite field $\mathbf{F}_{p^n}$ for a prime number p

---

Solution: $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p) = \langle \mathscr{F} \rangle$ is cyclic of order n, generated by the Frobenius automorphism $\mathscr{F} : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ given by $x \mapsto x^p$.

- an example of a field extension $F \subset E$ such that E is *not normal* over F.

Solution: If α is a root of $T^3 - 2$ then $\mathbf{Q}(\alpha)$ is not a normal extension of $\mathbf{Q}$. Indeed, the polynomial $T^3 - 2$ is irreducible over $\mathbf{Q}$, has a root in $\mathbf{Q}(\alpha)$, but does not split over $\mathbf{Q}(\alpha)$.

- for $a \in K$, describe the roots of $T^n - a \in K[T]$ in a splitting field of f over K

Solution: (I should have stipulated that K has characteristic $0 \ldots$) Let L be a splitting field for $T^n - 1$ over K and let $A \subset L^\times$ by the roots of $T^n - 1$ in L. Then A is a subgroup of $L^\times$ and is thus *cyclic*; choose a generator ω so that $A = \langle \omega \rangle$. (One says that ω is a primitive nth root of unity).
Now let E be a splitting field of $T^n - a$ over L and choose a root $\alpha \in E$ of $T^n - a$. Then $\alpha^n = a$ and for any $j \in \mathbf{Z}$ we have $(\omega^j)^n = a$. Thus $\alpha, \omega\alpha, \cdots, \omega^{n-1}\alpha$ are n distinct roots of $T^n - a$ and we conclude that

$$T^n - a = \prod_{j=0}^{n-1} (T - \omega^j \alpha)$$

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

1. Let L_1 and L_2 be splitting fields over K of the polynomial $f \in K[T]$. We have seen before that $L_1 \simeq L_2$. More precisely, there is an isomorphism $\phi : L_1 \to L_2$ for which $\phi(a) = a$ for all $a \in K$.
   Use ϕ to show that there is an isomorphism $\mathrm{Gal}(L_1/K) \xrightarrow{\sim} \mathrm{Gal}(L_2/K)$. (Be sure to show that the mapping you exhibit is in fact an isomorphism).

   Solution: We define a mapping

   $$\Lambda : \mathrm{Gal}(L_1/K) \xrightarrow{\sim} \mathrm{Gal}(L_2/K)$$

   by the rule:

   $$\Lambda(f) = \phi \circ f \circ \phi^{-1}$$

   for $f \in \mathrm{Gal}(L_1/K)$, and we define a mapping

   $$\Gamma : \mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1/K)$$

   by the rule

   $$\Gamma(g) = \phi^{-1} \circ g \circ \phi$$

   for $g \in \mathrm{Gal}(L_2/K)$. It is easy to see that $\Lambda \circ \Gamma$ is the identity on $\mathrm{Gal}(L_1/K$ and that $\Gamma \circ \Lambda$ is the identity on $\mathrm{Gal}(L_2/K)$.
   And it is straightforward to confirm that Λ is a group homomorhpism: For $f_1, f_2 \in \mathrm{Gal}(L_1/K)$, we have

   $$\Lambda(f_1 f_2) = \phi \circ f_1 \circ f_2 \circ \phi^{-1} = \phi \circ f_1 \circ \phi^{-1} \circ \phi \circ f_2 \circ \phi^{-1} = \Lambda(f_1)\Lambda(f_2).$$

   Thus Λ is an isomorphism of groups, as required.

2. Let ω be a root of $f(T) = \dfrac{T^5-1}{T-1} = T^4+T^3+T^2+T+1 \in \mathbf{Q}[T]$ in some splitting field of f over $\mathbf{Q}$.

   a. Explain why $\mathbf{Q}(\omega)$ is a normal separable extension of $\mathbf{Q}$.

   Solution: Since ω^j is a root of f for each $j \in \mathbf{Z}_{\geq 0}$ it follows that f splits over $\mathbf{Q}(\omega)$ and hence that $\mathbf{Q}(\omega)$ is a splitting field for f over $\mathbf{Q}$.
   This shows that $\mathbf{Q}(\omega)$ is *normal* over $\mathbf{Q}$. It is separable over $\mathbf{Q}$ since $\mathbf{Q}$ has characteristic 0. (Alternatively, we know that the extension is separable since it is the splitting field of the separable polynomial $T^n - 1$).

   b. Describe the group $\mathrm{Gal}(\mathbf{Q}(\omega)/\mathbf{Q})$. What is its *order*? What can you say about its *group structure*?

   Solution: The indicated Galois group is isomorphic to the group of units $(\mathbf{Z}/5\mathbf{Z})^\times$ in the field $\mathbf{F}_5 = \mathbf{Z}/5\mathbf{Z}$. Indeed, the roots of f are precisely the elements ω^j where $j \in \mathbf{Z}$ and $j \not\equiv 0 \pmod 5$, and for each such j there is an automorphism σ_j of $\mathbf{Q}(\omega$ with the property that $\sigma_j(\omega) = \omega^j$.
   The mapping $(\mathbf{Z}/5\mathbf{Z})^\times \to \mathrm{Gal}(\mathbf{Q}(\omega)/\mathbf{Q})$ given by $j+5\mathbf{Z} \mapsto \sigma_j$ is an isomorphism. Now, the group $(\mathbf{Z}/5\mathbf{Z})^\times$ has order 4; since it is the multiplicative group of the finite field $\mathbf{F}_5 = \mathbf{Z}/5\mathbf{Z}$, it is a *cyclic* group.

3. Let K be a finite field and let $a \in K$ be an element for which $f = T^3 - a \in K[T]$is *irreducible*. Let $L = K(\sqrt[3]{a})$ be a splitting field for f over K.
   Using results from the lectures, Prove the following: if $g \in K[T]$ is an irreducible polynomial of degree 3, then g splits over L.

   Solution: First of all, recall that any finite extension of a finite field is a normal extension. This show that f indeed splits over $L = K(\sqrt[3]{a})$ so that L is a splitting field for f.
   Now, suppose that g is any irreducible polynomial of degree 3 over K. Let E be a splitting field for g over the field L and let $\beta \in E$ be a root of g.
   Then $K(\beta) \subseteq E$ is an extension of degree 3. Moreover, since $K(\beta)$ is a normal extension of K, g splits over $K(\beta)$.
   Now, according to results from the notes, any two finite fields of the same order are isomorphic. In fact, we know that any two subfields of E with the same order actually coincide. Thus $L = K(\beta)$.
   Since g splits over $K(\beta)$, it follows that g splits over $L = K(\sqrt[3]{a})$ as required.

4. Let $K = \mathbf{Q}(X)$ be the field of rational functions over $\mathbf{Q}$. Observe that

$$L = \mathbb{Q}(X)(\sqrt{X}, \sqrt{X+1})$$

   is a splitting field over $\mathbb{Q}(X)$ of the polynomial

$$(T^2 - X)(T^2 - (X+1)) \in \mathbf{Q}(X)[T] = K[T]).$$

   a Show that $[L : \mathbb{Q}(X)] = 4$ and deduce that $\mathrm{Gal}(L/\mathbf{Q})(X)$ has order 4.

Solution: We need to know that $h = T^2 - (X+1)$ remains irreducible over $\mathbf{Q}(X)(\sqrt{X})$. For this, it is enough to argue that h has no root in $\mathbf{Q}(X)(\sqrt{X})$. Suppose that contrary, namely that $\alpha = f + g\sqrt{X} \in \mathbf{Q}(X)(\sqrt{X})$ is a root of h where $f, g \in \mathbf{Q}(X)$. Then

$$X + 1 = h^2 = f^2 + Xg^2 + 2fg\sqrt{X}$$

This shows that $fg = 0$ so that either $f = 0$ or $g = 0$.
If $f = 0$ then $X + 1 = Xg^2$. Writing $g = \frac{a}{b}$ for relatively prime polynomials $a, b \in \mathbf{Q}[X]$ we find that $(X+1)b^2 = Xa^2$ which is impossible since X has even multiplicity as a factor on the LHS, and odd multiplicity as a factor on the RHS.
If $g = 0$ then $X + 1 = f^2$ which is impossible since we know that $T^2 - (X+1)$ is irreducible by Eisenstein.
Conclude that $T^2 - (X+1)$ remains irreducible over $\mathbf{Q}(X)(\sqrt{X})$; this shows that $[\mathbf{Q}(\sqrt{X}, \sqrt{X+1}) : \mathbf{Q}(X)] = 4$.
Since $\mathbf{Q}(\sqrt{X}, \sqrt{X+1})$ is a splitting field for the polynomial $(T^2 - X)(T^2 - (X+1))$, it is a normal separable extension of $\mathbf{Q}(X)$; thus the fundamental theorem of Galois theory implies that $\mathrm{Gal}(L/\mathbf{Q}(X))$ has order 4.

b. Recall that any group of order 4 is either cyclic or isomorphic to the group

$$\mathscr{K} = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

Decide whether $\Gamma = \mathrm{Gal}(L/\mathbf{Q})$ is cyclic or is isomorphic to $\mathscr{K}$.

Solution: Γ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

We have seen above that $[L : \mathbf{Q}(X)(\sqrt{X})] = 2$ and $[L : \mathbf{Q}(X)(\sqrt{X+1})] = 2$ and we know that L is normal over $\mathbf{Q}(X)$ and hence normal over $\mathbf{Q}(X)(\sqrt{X})$ and over $\mathbf{Q}(X)(\sqrt{X+1})$.
It follows that the groups $\mathrm{Gal}(L/\mathbf{Q}(X)(\sqrt{X}))$ and $\mathrm{Gal}(L/\mathbf{Q}(X)(\sqrt{X+1}))$ each have order 2.
Let $\sigma \in \mathrm{Gal}(L/\mathbf{Q}(X)(\sqrt{X}))$ and $\tau \in \mathrm{Gal}(L/\mathbf{Q}(X)(\sqrt{X+1}))$ be non-trivial elements. Then $\sigma(\sqrt{X+1}) = -\sqrt{X+1}$ and $\tau(\sqrt{X}) = -\sqrt{X}$.
We claim that Γ has 3 elements of order 2, namely σ, τ and $\sigma\tau$. Since $|\Gamma| = 4$ this implies that Γ is not cyclic and hence is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
To prove the claim, we need to argue that $\sigma\tau$ is not equal to σ or to τ. For this, we compute:

$$\sigma\tau(\sqrt{X}) = \sigma(-\sqrt{X}) = -\sqrt{X}$$

since σ is the identity on $\mathbf{Q}(X)(\sqrt{X})$.
and

$$\sigma\tau(\sqrt{X+1}) = \sigma(\sqrt{X+1}) = -\sqrt{X+1}$$

since τ is the identity on $\mathbf{Q}(X)(\sqrt{X+1})$.
This calculation shows that $\sigma\tau \neq 1$ and hence that σ, τ and $\sigma\tau$ are all distinct, as required.

c. By finding all subgroups of Γ, use the fundamental theorem of Galois theory to list all intermediate fields of the extension $\mathbb{Q}(X) \subseteq L = \mathbb{Q}(X)(\sqrt{X}, \sqrt{X+1})$.

Solution: The full list of proper non-trivial subgroups of $\Gamma \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is $\langle\sigma\rangle, \langle\tau\rangle$ and $\langle\sigma\tau\rangle$. Now,

- $\mathbf{Q}(X)(\sqrt{X})$ is the fixed field $L^{\langle\sigma\rangle}$.
- $\mathbf{Q}(X)(\sqrt{X+1})$ is the fixed field $L^{\langle\tau\rangle}$.
- $\mathbf{Q}(X)(\sqrt{X(X+1)})$ is the fixed field $L^{\langle\sigma\tau\rangle}$.
  To confirm this third assertion, notice that $\sqrt{X(X+1)} = \sqrt{X}\sqrt{X+1}$ is certainly fixed by $\sigma\tau$ and since the polynomial is $T^2 - X(X+1)$ is irreducible by Eisenstein, it is the minimal polynomial of $\sqrt{X}\sqrt{X+1}$ over $\mathbf{Q}(X)$ so that $[\mathbf{Q}(X)(\sqrt{X(X+1)}) : \mathbf{Q}(X)] = 2$. Hence $\mathbf{Q}(X)(\sqrt{X(X+1)}) = L^{\langle\sigma\tau\rangle}$ by the fundamental theorem.

5. For $n \in \mathbf{Z}_{\geq 0}$, let $\mathscr{P}_n = \{f \in K[T] \mid \deg f < n\}$, and note that $\dim_K \mathscr{P}_n = n$.
   Fix a polynomial $g \in K[T]$ of degree ≤ 2, say $g = a_0 + a_1 T + a_2 T^2$ for $a_0, a_1, a_2 \in K$. Show that multiplication by g defines a mapping

$$\lambda_g : \mathscr{P}_n \to \mathscr{P}_{n+2};$$

   Thus $\lambda_g(h) = gh$ for $h \in \mathscr{P}_n$.
   If $n = 3$, find the matrix representing the linear mapping λ_g with respect to the monomial bases of $\mathscr{P}_3$ and $\mathscr{P}_5$.

Solution: The matrix M of the linear transformation λ_g is a 5×3 matrix. Since $\lambda_g(1) = a_0 + a_1 T + a_2 T^2$, $\lambda_g(T) = a_0 T + a_1 T^2 + a_2 T^3$ and $\lambda_g(T^2) = a_0 T^2 + a_1 T^3 + a_2 T^4$ we see that

$$M = \begin{pmatrix} a_0 & 0 & 0 \\ a_1 & a_0 & 0 \\ a_2 & a_1 & a_0 \\ 0 & a_2 & a_1 \\ 0 & 0 & a_2 \end{pmatrix}$$

6. Let L be a splitting field over $\mathbf{Q}$ of the polynomial $T^3 - 7$.

   a. Let $\omega \in L$ be root of $\dfrac{T^7 - 1}{T - 1}$. Show that $\mathrm{Gal}(L/\mathbf{Q}(\omega))$ is cyclic, isomorphic to $\langle\sigma\rangle$. What is the order of this group (i.e. what is the order of σ)?

Solution: Typo: I should have written that ω is a root of $\dfrac{T^3 - 1}{T - 1}$.

Also: Compare this problem with the "non-abelian Galois group" example given in solutions to section III above.
$L = \mathbf{Q}(\omega, \alpha)$ where α is a root of $T^3 - 7$ is a splitting field for $f = T^3 - 7$.
Moreover L is a normal extension of $\mathbf{Q}(\omega)$ of degree 3, hence $\mathrm{Gal}(L/\mathbf{Q}(\omega)$ is cyclic of order 3, generated by an element σ satisfying $\sigma(\alpha) = \omega\alpha$.
It is straightforward to check that σ^3 is the identity. Indeed, σ is already the identity on $\mathbf{Q}(\omega)$, so it suffices to show that $\sigma^3(\alpha) = \alpha$. But

$$\sigma^3(\alpha) = \sigma^2(\omega\alpha) = \omega\sigma^2(\alpha) = \omega^2\sigma(\alpha) = \omega^3\alpha = \alpha$$

b. Let $\alpha \in L$ be a root of $T^3 - 7$. Show that $\mathrm{Gal}(L/\mathbf{Q}(\alpha)$ is cyclic, isomorphic to $\langle\tau\rangle$. What is the order of this group (i.e. what is the order of τ)?

Solution: L is a normal extension of $\mathbf{Q}(\alpha)$ of degree 2. Hence $\mathrm{Gal}(L/\mathbf{Q}(\alpha)$ is cyclic of order 2, generated by an element τ satsifying $\tau(\omega) = \omega^2$.
It is straightforward to check that τ^2 is the identity. Indeed, since τ is the identity on $\mathbf{Q}(\alpha)$ it is enough to argue that $\tau^2(\omega) = \omega$).
But

$$\tau^2(\omega) = \tau(\omega^2) = \tau(\omega)\tau(\omega) = \omega^2\omega^2 = \omega^4 = \omega.$$

c. Prove that $\tau\sigma\tau = \sigma^3$ in $\mathrm{Gal}(L/\mathbf{Q})$.

Solution: Typo: That should read $\tau\sigma\tau = \sigma^2$, not σ^3! ("really" it is σ^{-1}).

We need to prove that $\tau\sigma\tau$ and σ^3 agree on ω and on α.

- on ω:

$$\tau\sigma\tau(\omega) = \tau(\omega^2) = \omega^4 = \omega$$

$$\sigma^2(\omega) = \omega.$$

- on α:

$$\tau\sigma\tau(\alpha) = \tau\sigma(\alpha) = \tau(\omega\alpha) = \tau(\omega)\tau(\alpha) = \omega^2\alpha.$$

$$\sigma^2(\alpha) = \sigma(\omega\alpha) = \omega\sigma(\alpha) = \omega^2\alpha$$

Note of course that since $|\Gamma| = 6$ the identity in (c) shows that Γ is isomorphic to the dihedral group D_3 of order 6.