Math 206C: Algebra

Midterm 2: Solutions

Friday, May 21, 2021.

Problems

1. Prove that the polynomial $f(x) = 1 + \frac{x}{1} + \frac{x^2}{2} + \cdots + \frac{x^n}{n!} \in \mathbb{Q}[x]$ has no multiple roots in $\mathbb{C}$.

   Solution: A polynomial $f(x)$ has α as a multiple root if and only if α is a root of both $f(x)$ and its derivative $f'(x)$. We have

   $$f'(x) = 1 + \frac{x}{1} + \frac{x^2}{2!} + \cdots + \frac{x^{n-1}}{(n-1)!}.$$

   We see that if α is a root of both $f(x)$ and $f'(x)$ then

   $$f(\alpha) - f'(\alpha) = \frac{\alpha^n}{n!} = 0,$$

   which implies $\alpha = 0$. But clearly, $f(\alpha) = 1 \neq 0$. Therefore, $f(x)$ does not have any multiple roots in $\mathbb{C}$.

2. Suppose that V is a finite dimensional vector space and $T\colon V \to V$ is a linear transformation that has characteristic polynomial which is irreducible over $\mathbb{Q}$.
   Show that the matrix of T (in any basis of V) can be diagonalized **over the field** $\mathbb{C}$.

   Solution: We recall that if A is a matrix with entries in a field F that contains all of the eigenvalues of A, then A can be diagonalized over F if all of the eigenalues of A are distinct.

   Let A be the matrix of T with respect to some basis $\mathcal{B}$ of V. The characteristic polynomial of T is the characteristic polynomial of A, $c_A(x)$. This is an irreducible polynomial in $\mathbb{Q}[x]$.

   If F is a perfect field, every irreducible polynomial in $F[x]$ is separable over F. Every field of characteristic 0 is perfect. So $c_A(x)$ has distinct roots in a algebraic closure of $\mathbb{Q}$.

   Recall that $\mathbb{C}$ is algebraically closed, and $\overline{\mathbb{Q}} \subset \mathbb{C}$ is an algebraic closure of $\mathbb{Q}$. We conclude that $c_A(x)$ has distinct roots in $\mathbb{C}$, so A can be diagonalized over $\mathbb{C}$.

3. Factor $x^4 + 1 \in F[x]$ and find the splitting field over F if the ground field F is:

   $$(a)\ \mathbb{Q}, \qquad (b)\ \mathbb{F}_2, \qquad (c)\ \mathbb{R}.$$

   Solution: We note that $x^4 + 1 = \Phi_4(x)$ and we know that $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$ for any n. The roots of $x^4 + 1$ are the primitive 8^{th} roots of unity. One such root is

   $$\zeta_8 = e^{2\pi i/8} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i.$$

We see that the splitting field of this polynomial is $\mathbb{Q}(\zeta_8)$.

Over $\mathbb{F}_2$ we see that

$$x^4+1=\left(x^2\right)^2+1^2=(x^2+1)^2=\left((x+1)^2\right)^2=(x+1)^4.$$

The splitting field over $\mathbb{F}_2$ of this polynomial is $\mathbb{F}_2$.

We see that the splitting field of x^4+1 over $\mathbb{R}$ includes ζ_8, which means it also includes $\zeta_8^2=i$. So this splitting field includes $\mathbb{R}(i)=\mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, it contains all of the roots of x^4+1. So $\mathbb{C}$ is the splitting field of x^4+1 over $\mathbb{R}$.

Since $\mathbb{C}$ is a quadratic extension of a field of characteristic 0, it is a Galois extension. The nontrivial Galois element given by complex conjugation. The roots of $m_{\zeta_8,\mathbb{R}}(x)$ are the distinct Galois conjugates of ζ_8. Therefore,

$$m_{\zeta_8,\mathbb{R}}(x)=(x-\zeta_8)(x-\overline{\zeta_8})=x-(\zeta_8+\overline{\zeta_8})x+\zeta_8\overline{\zeta_8}.$$

It is helpful to note that $\overline{\zeta_8}=\zeta_8^7$, and using the expression for ζ_8 given above, we see that

$$m_{\zeta_8,\mathbb{R}}(x)=x^2-\sqrt{2}x+1.$$

The remaining two roots of x^4+1 are $-\zeta_8$ and $-\overline{\zeta_8}$. So,

$$m_{\zeta_8^3,\mathbb{R}}(x)=(x+\zeta_8)(x+\overline{\zeta_8})=x^2+\sqrt{2}x+1.$$

So

$$x^4+1=(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1).$$

4. Let p be prime and $\mathbb{F}_p\subset\mathbb{F}_{p^n}$ be a degree $n>1$ extension of finite fields. Consider the Frobenius automorphism $\Phi\colon\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ sending α to α^p. Show that Φ is $\mathbb{F}_p$-linear, that its minimal polynomial $m_\Phi(x)$ has degree n, and then compute the minimal polynomial. **Solution**: We first note that for any $\alpha,\beta\in\mathbb{F}_p$, we have

$$\Phi(a+b)=(a+b)^p=a^p+b^p.$$

This statement holds in any ring of characteristic p, the proof uses the Binomial Theorem:

$$(a+b)^p=\sum_{k=0}^{p}\binom{p}{k}a^kb^{p-k}=a^p+b^p+\sum_{k=1}^{p-1}\binom{p}{k}a^kb^{p-k}.$$

We now need only note that for each $k\in\{1,\ldots,p-1\}$, we have $\binom{p}{k}=\frac{p!}{k!(p-k)!}$ is divisible by p because the numerator is, but the denominator is the product of two terms, neither of which is divisible by p.

We now note that $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_p$ with the scalar multiplication given by the standard multiplication in $\mathbb{F}_{p^n}$. For any $c \in \mathbb{F}_p$ and $\alpha \in \mathbb{F}_{p^n}$ we have

$$\Phi(c \cdot \alpha) = c^p \cdot \alpha^p = c \cdot \Phi(\alpha),$$

since $c^p = c$. Therefore, Φ is $\mathbb{F}_p$-linear.

Suppose that

$$m_\Phi(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_p[x].$$

Then

$$\Phi^m + a_{m-1}\Phi^{m-1} + \cdots + a_1\Phi + a_0 I = 0$$

as a linear transformation from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. That is,

$$\alpha^{p^m} + a_{m-1}\alpha^{p^{m-1}} + \cdots + a_1\alpha^p + a_0 = 0$$

for all $\alpha \in \mathbb{F}_{p^n}$. This is not possible if $m < n$, because then we would have a nonzero polynomial

$$x^{p^m} + a_{m-1}x^{p^{m-1}} + \cdots + a_1 x^p + a_0$$

of degree p^m with at least p^n roots in $\mathbb{F}_{p^n}$.

Therefore, we see that the degree of $m_\Phi(x)$ is at least n. We see that it is exactly n by noting that

$$\alpha^{p^n} - \alpha = 0$$

for all $\alpha \in \mathbb{F}_{p^n}$, so $\Phi^n - I = 0$ as a linear transformation on $\mathbb{F}_{p^n}$. This implies $m_\Phi(x) = x^n - 1$.

5. Let n be a positive integer. Prove that the n^{th} cyclotomic polynomial $\Phi_n(x)$ has integer coefficients.

Solution: The n^{th} cyclotomic polynomial $\Phi_n(x)$ is the monic polynomial whose roots are the primitive n^{th} roots of unity. We prove this statement by induction on n. For $n = 1$ we note that $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$.

We recall that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. We see that this is true by comparing the roots on both sides of the equation and noting that every n^{th} root of unity is a primitive d^{th} root of unity for some $d \mid n$ (d is the order of this root in the group of n^{th} roots of unity).

We assume that the statement is true for all $m < n$. We see that

$$x^n - 1 = \Phi_n(x) \cdot \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x).$$

Let $g(x) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$.

By induction, $g(x) \in \mathbb{Z}[x]$. Therefore, we see that $g(x)$ divides $x^n - 1$ in $\mathbb{Q}(\zeta)[x]$. By uniqueness of the remainder when applying the division algorithm in field extensions, since $x^n - 1,\ g(x) \in \mathbb{Q}[x]$, we see that $g(x) \mid x^n - 1$ in $\mathbb{Q}[x]$. This proves that $\Phi_n(x) \in \mathbb{Q}[x]$.

We note that $x^n - 1, \Phi_n(x)$, and $g(x)$ are all monic polynomials. By Gauss' lemma, we conclude that in fact, $\Phi_n(x) \in \mathbb{Z}[x]$ (since the other two polynomials are).

6. Let p be an odd prime. How many subfields of $\mathbb{F}_{p^{12}}$ are there?
   Solution: For each p and each n, $\mathbb{F}_{p^n}$ is a Galois extension of $\mathbb{F}_p$ with $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$. Every subfield of $\mathbb{F}_{p^n}$ contains its prime subfield $\mathbb{F}_p$. By the Galois correspondence there is a bijection between subfields E of $\mathbb{F}_{p^n}$ containing $\mathbb{F}_p$ and subgroups of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Subgroups of $\mathbb{Z}/n\mathbb{Z}$ are in bijection with divisors d of n. So, the number of subfields of $\mathbb{F}_{p^n}$ is the number of divisors of n. The divisors of 12 are $\{1, 2, 3, 4, 6, 12\}$, so there are 6 subfields of $\mathbb{F}_{p^{12}}$.

7. Does there exist a field F and an extension K/F with $[K\colon F] = 2$ that is **not** a Galois extension? Either give an example and explain why it has this property, or prove that no example exists.
   Solution: We proved that a degree 2 extension of a field F of characteristic **not equal to** 2 is Galois because it is a splitting over F of a **separable** polynomial over F. So, we want to find a quadratic polynomial over a field of characteristic 2 that is **not separable**.

   Consider $F = \mathbb{F}_2(u)$ and $f(x) = x^2 - u \in F[x]$. This polynomial is irreducible in $F[x]$ since it is Eisenstein at u (really, Eisenstein's criterion shows that it is irreducible in $\mathbb{F}_2[u][x]$ and then Gauss' lemma shows that it is irreducible in $F[x]$). This polynomial is not separable since $f'(x) = 2x = 0$. Therefore, the field we get by adjoining a root of this polynomial to F, $F(u^{1/2}) = \mathbb{F}_2(u^{1/2})$ is not separable over F, so it is not a Galois extension of F.

8. Let $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ and $F = \mathbb{Q}(\sqrt{-3})$. Is K/F a Galois extension? Justify your answer.
   Solution: This is a Galois extension. First we note that $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$, so $K = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. We see that K is a splitting field of $x^3 - 2$ over $\mathbb{Q}$ by noting that it contains all of the roots of $x^3 - 2$, and that $\mathbb{Q}(\sqrt[3]{2})$ does not.

   We now need only note that if K/F is a Galois extension, then for any subfield E of K containing F, K/E is a Galois extension.

9. Let K be a field and H be a subgroup of $\mathrm{Aut}(K)$.
   Recall that K^H denotes the subfield of K consisting of elements fixed by every $\sigma \in H$.
   Is it true that $H \subseteq \mathrm{Aut}(K/K^H)$?
   Either prove this statement or give a counterexample.
   Solution: Let $\sigma \in H$. It is clear that σ is an automorphism of K so we need only show that σ fixes every element of K^H. If $\alpha \in K^H$, then α is fixed by every element of H, so in particular, $\sigma(\alpha) = \alpha$.