Math 206C: Algebra

Final Exam Solutions

Thursday, June 10, 2021.

Problems

1. Let V be a vector space over $\mathbb{Q}$ of dimension at most $p-2$ where p is prime. Let T be a linear transformation on V such that $T^p = I$ (where I denotes the identity linear transformation). Show that $T = I$.

   Solution: Since $T^p - I = 0$ the minimal polynomial of T divides $x^p - 1$. We know that $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$. Also, $x^{p-1} + \cdots + x + 1 = \Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$. (We can prove this by applying Eisenstein's criterion to $\Phi_p(x+1)$, or we can note that we proved that $\Phi_n(x)$ is irreducible for all n.)

   Since the dimension of V is the degree of the characteristic polynomial of T, which is greater than or equal to the degree of the minimal polynomial of T, the only possibility for the minimal polynomial of T is $x-1$. The unique linear transformation with minimal polynomial $x-1$ is the identity.

2. Determine up to similarity all 3×3 matrices in $\mathrm{GL}_3(\mathbb{Q})$ of order **exactly** 6.

   Solution: A matrix $A \in \mathrm{GL}_3(\mathbb{Q})$ with order dividing 6 satisfies $A^6 - I = 0$. Therefore, the minimal polynomial of A divides

   $$x^6 - 1 = (x-1)(x^2+x+1)(x+1)(x^2-x+1).$$

   The two quadratic polynomials here are irreducible in $\mathbb{Q}[x]$ since they are $\Phi_3(x)$ and $\Phi_6(x)$, or you can see this by applying the quadratic formula.

   The minimal polynomial of A, $m_A(x)$, divides the characteristic polynomial of A, $c_A(x)$, and $\deg(c_A(x)) = 3$. Every invariant factor of A divides $m_A(x)$, and since $c_A(x)$ is the product of all the invariant factors, we cannot have $m_A(x)$ being one of the two irreducible quadratic polynomials.

   Therefore, $m_A(x)$ must be one of the following possibilities:

   (a) $x-1$
   (b) $x+1$
   (c) $(x-1)(x+1)$
   (d) $(x-1)(x^2+x+1)$
   (e) $(x+1)(x^2+x+1)$

(f) $(x-1)(x^2-x+1)$

(g) $(x+1)(x^2-x+1)$.

We are not looking to classify matrices of order dividing 6, but matrices of order **exactly** 6. This means that $m_A(x)$ cannot divide x^3-1 or x^2-1. Therefore, $m_A(x)$ must be one of the following possibilities:

(a) $(x+1)(x^2+x+1)$

(b) $(x-1)(x^2-x+1)$

(c) $(x+1)(x^2-x+1)$.

For each of these three possibilities, we see that $m_A(x) = c_A(x)$. The companion matrix of $m_A(x)$ is an element in the corresponding similarity class. We conclude that every $A \in \mathrm{GL}_3(\mathbb{Q})$ of order exactly 6 is similar to one of:

$$\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & -2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -2 \\ 0 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

3. Let $F \subseteq K \subseteq L$ be fields and suppose that L/F is finite. Prove that $[L\colon F] = [L\colon K]\cdot[K\colon F]$.

Solution: We first note that L/F being finite implies that L/K is finite and K/F is finite. Suppose $[K\colon F] = m$ and $[L\colon K] = n$. Let $\{\alpha_i\}_{i=1,\ldots,m}$ be a basis for K/F and $\{\beta_j\}_{j=1,\ldots,n}$ be a basis for L/K. We show that $\{\alpha_i\beta_j\}$ where $i \in [1,m]$ and $j \in [1,n]$ is a basis for L/F.

Let $\gamma \in L$. Since $\{\beta_j\}_{j=1,\ldots,n}$ is a basis for L/K, we know that γ can be written uniquely as

$$\gamma = \sum_{j=1}^{n} b_j\beta_j, \quad \text{where } b_j \in K.$$

Since $\{\alpha_i\}_{i=1,\ldots,m}$ is a basis for K/F, each b_j can be written uniquely as

$$b_j = \sum_{i=1}^{m} c_{ij}\alpha_i, \quad \text{where } c_{ij} \in F.$$

Using these expressions for b_j we see that

$$\gamma = \sum_{j=1}^{n} b_j\beta_j = \sum_{j=1}^{n}\sum_{i=1}^{m} c_{ij}\alpha_i\beta_j.$$

We see that $\{\alpha_i\beta_j\}$ span L as a vector space over F.

To see that they are linearly independent, note that since $\{\alpha_i\}_{i=1,\ldots,m}$ is a basis for K/F, the only solution to

$$0 = \sum_{i=1}^{m} c_i \alpha_i,$$

is given by $c_1, \ldots, c_m = 0$. Since $\{\beta_j\}_{j=1,\ldots,n}$ is a basis for L/K, the only solution to

$$0 = \sum_{j=1}^{n} b_j \beta_j$$

is given by $b_1, \ldots, b_n = 0$. Therefore,

$$0 = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} c_{ij} \alpha_i \right) \beta_j$$

implies that for every j

$$\left(\sum_{i=1}^{m} c_{ij} \alpha_i \right) = 0.$$

This implies that for fixed j, each $c_{ij} = 0$, so all $c_{ij} = 0$.

4. Let K/F be a field extension and $\sigma \in \mathrm{Aut}(K/F)$ be an automorphism of K fixing F. Suppose $f(x) \in F[x]$ and $\alpha \in K$.

   (a) Prove that $\sigma(f(\alpha)) = f(\sigma(\alpha))$.
   Solution: The proof is a computation. Let

   $$f(x) = a_n x^n + \cdots a_1 x + a_0, \quad a_0, \ldots, a_n \in F.$$

   Then we have

   $$\begin{aligned} \sigma(f(\alpha)) &= \sigma\left(a_n \alpha^n + \cdots a_1 \alpha + a_0\right) \\ &= \sigma\left(a_n \alpha^n\right) + \cdots + \sigma(a_0) \\ &= \sigma(a_n)\sigma(\alpha^n) + \cdots + \sigma(a_0) \\ &= a_n \sigma(\alpha)^n + \cdots + a_1 \sigma(\alpha)^1 + a_0 \\ &= f(\sigma(\alpha)). \end{aligned}$$

   We used the fact that σ fixes every element of F and that σ is a homomorphism.

(b) Prove that σ permutes the set of roots of $f(x)$ in K.

Solution: If $f(\alpha) = 0$ then $\sigma(f(\alpha)) = \sigma(0) = 0$, since σ is an automorphism. By the previous part, $0 = f(\sigma(\alpha))$, so $\sigma(\alpha)$ is a root of $f(x)$. Since σ is an automorphism of K, $\alpha \in K$ implies $\sigma(\alpha) \in K$.

Since σ is an automorphism of K it is an injective function on K. The set of roots of $f(x)$ in K is finite. We have seen that σ maps elements of this finite set to elements of this finite set. An injective map from a **finite** set to itself is automatically a bijection. So σ permutes the roots of $f(x)$ in K.

5. (a) State the Primitive Element Theorem.

Solution: Suppose K/F is a finite separable extension. Then K/F is a simple extension. That is, there exists some $\alpha \in K$ such that $K = F(\alpha)$.

(b) Define what if means for a field F of characteristic p to be perfect.

Solution: F is perfect if every element of F is a p^{th} power in F. That is, for every $\alpha \in F$, there exists $\beta \in F$ such that $\alpha = \beta^p$.

(c) Let F be a field. Define what it means for a field to be an algebraic closure of F.

Solution: $\overline{F}$ is an algebraic closure of F if $\overline{F}$ is algebraic over F and every polynomial in $F[x]$ splits completely in $\overline{F}[x]$.

6. Let F be any field. Prove that if K/F is a finite extension, then it is an algebraic extension.

Solution: Suppose $[K\colon F] = n$. Let $\alpha \in K$. We claim that α satisfies a polynomial in $F[x]$ of degree at most n.

Consider the $n+1$ elements of $K : 1, \alpha, \alpha^2, \ldots, \alpha^n$. Since K is an n-dimensional vector space over F these elements must be linearly dependent over F. That is, there exist $a_0, \ldots, a_n \in F$ not all 0 such that

$$a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n = 0.$$

That is, α is a root of the polynomial

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x].$$

Since α is a root of a polynomial in $F[x]$, α is algebraic over F.

7. Determine the Galois group of the polynomial $(x^3 - x + 1)(x^2 - 2)$ over $\mathbb{Q}$ as an abstract group.

Solution: We first determine the Galois group of $f_1(x) = x^3 - x + 1$ over $\mathbb{Q}$. This polynomial is irreducible because it has no roots in $\mathbb{Q}$. (By the Rational Root Theorem, the only possible roots would be ± 1.) Therefore the Galois group of this polynomial is isomorphic to a transitive subgroup of S_3, so it is either S_3 or $A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

The discriminant of this polynomial is $D = -4 \cdot (-1)^3 - 27 \cdot 1^2 = -23$. This is not a square in $\mathbb{Q}$. Therefore, $\mathrm{Gal}(f_1)$ is not contained in A_3, so it must be S_3. Let E be the splitting field of $f_1(x)$ over $\mathbb{Q}$.

The splitting field of $f_2(x) = x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$. The splitting field of $f_1(x)f_2(x)$ is the composite of E and $\mathbb{Q}(\sqrt{2})$. By the Fundamental Theorem of Galois Theory, since there is a unique subgroup of S_3 of index 2, there is a unique quadratic subfield of E containing $\mathbb{Q}$. It is $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{-23})$.

It is clear that $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{-23})$. Therefore, $E \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}$. We now apply that fact that if K_1, K_2 are Galois extensions of F with $K_1 \cap K_2 = F$ then $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$. We conclude that the Galois group of $f_1(x)f_2(x)$ is isomorphic to $S_3 \times \mathbb{Z}/2\mathbb{Z}$.

8. Let K be the splitting field over $\mathbb{Q}$ of $x^8 - 1$.

   (a) Find $[K\colon \mathbb{Q}]$.
   Solution: We know that $K = \mathbb{Q}(\zeta_8)$ where $\zeta_8 = e^{2\pi i/8}$. The minimal polynomial for ζ_8 over $\mathbb{Q}$ is $\Phi_8(x) = x^4 + 1$. Therefore, $[K\colon \mathbb{Q}] = 4$.
   It will be useful later in this problem, so we note that

$$e^{2\pi i/8} = \cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2} + i\sqrt{2}}{2}.$$

   (b) Describe the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ both as an abstract group and as a set of automorphisms.
   Solution: We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ where the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ are determined by where they send ζ_n. For each $1 \leq a \leq n$ with $\gcd(a, n) = 1$ we have an automorphism $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ where $\sigma_a(\zeta_n) = \zeta_n^a$. So in this example, we have $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \{1 = \sigma_1, \sigma_3, \sigma_5, \sigma_7\}.$$

   (c) Find explicitly all subgroups of G and the corresponding subfields of K under the Galois correspondence.
   Solution: It is helpful to have a different description of K. It is clear $\mathbb{Q}(\sqrt{2}, i)$ is a degree 4 Galois extension with $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ where

$$\sigma\colon \begin{cases} \sqrt{2} & \mapsto -\sqrt{2} \\ i & \mapsto i \end{cases} \qquad \tau\colon \begin{cases} \sqrt{2} & \mapsto \sqrt{2} \\ i & \mapsto -i \end{cases}.$$

   It is clear that $K = \mathbb{Q}(\sqrt{2}+\sqrt{2}i) \subseteq \mathbb{Q}(\sqrt{2}, i)$. None of $\{\sigma, \tau, \sigma\tau\}$ fix the element $\sqrt{2}+\sqrt{2}i$, so K corresponds to the trivial subgroup under the Galois correspondence. Therefore, $K = \mathbb{Q}(\sqrt{2}, i)$.

With this description it is easy to compute fixed fields. The fixed field of G is $\mathbb{Q}$ and the fixed field of the trivial subgroup is $\mathbb{Q}(\sqrt{2}, i)$. The fixed field of $\langle\sigma\rangle$ is $\mathbb{Q}(i)$. The fixed field of $\langle\tau\rangle$ is $\mathbb{Q}(\sqrt{2})$. The fixed field of $\langle\sigma\tau\rangle$ is $\mathbb{Q}(i\sqrt{2})$. Since these are all the subgroups of G, these are all the fixed fields.

9. Determine the Galois group of the splitting field of the polynomial $x^3 + 2$ over $\mathbb{F}_3$, over $\mathbb{F}_7$, and over $\mathbb{F}_{11}$.

   Solution: In order to answer this question we factor this cubic polynomial over $\mathbb{F}_3$, over $\mathbb{F}_7$, and over $\mathbb{F}_{11}$. It is helpful to recall that a cubic is irreducible if and only if it does not have any roots. We will also use the fact that any degree n extension of $\mathbb{F}_p$ is isomorphic to $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

   Since $(a+b)^3 = a^3 + b^3$ in $\mathbb{F}_3$ and $2^3 = 2$ we have $x^3 + 2 = (x+2)^3$ over $\mathbb{F}_3$. Therefore, the splitting field of $x^3 + 2$ over $\mathbb{F}_3$ is $\mathbb{F}_3$ and the Galois group is trivial.

   Taking cubes of the integers from 1 to 6 shows that x^3+2 has no roots in $\mathbb{F}_7$, so it is irreducible. Therefore, the splitting field is a degree 3 extension of $\mathbb{F}_7$. This is a Galois extension with Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

   Taking cubes of small integers we see that $4^3 + 2 = 66 \equiv 0 \pmod{11}$, so 4 is a root of $x^3 + 2$ in $\mathbb{F}_{11}$. We have
   $$x^3 + 2 = (x-4)(x^2 + 4x + 5).$$
   We check that $x^2 + 4x + 5$ is irreducible in $\mathbb{F}_{11}$ by computing its discriminant: $\sqrt{4^2 - 4 \cdot 5} = \sqrt{-4}$. We see that -4 is not a square in $\mathbb{F}_{11}$. Therefore the splitting field is degree 2 over $\mathbb{F}_{11}$. Its Galois group is cyclic, isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

10. Fix a prime p. For all positive integers m and n, let $f(m,n)$ be the number of nonzero ring homomorphisms from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^n}$.
    Note: For this question you should assume that a ring homomorphism must take 1 to 1.

    (a) What is $f(m,6)$?
    Solution: The kernel of a ring homomorphism is an ideal. The only ideals of a field F are 0 and F. Since a ring homomorphism must take the identity to the identity, the kernel cannot be F.
    We need only count injective ring homomorphisms from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^6}$. By the First Isomorphism Theorem, in this case $\mathbb{F}_{p^m}$ is isomorphic to its image. Therefore, $f(m,6)$ is nonzero implies that $\mathbb{F}_{p^6}$ has a subfield isomorphic to $\mathbb{F}_{p^m}$. This occurs if and only if $m \mid 6$. In this case, there is a unique subfield of $\mathbb{F}_{p^6}$ isomorphic to $\mathbb{F}_{p^m}$.
    Suppose $m \mid 6$. We need only count isomorphisms from $\mathbb{F}_{p^m}$ to the unique subfield of $\mathbb{F}_{p^6}$ isomorphic to $\mathbb{F}_{p^m}$. Such an isomorphism can be identified with an automorphism of $\mathbb{F}_{p^m}$ fixing $\mathbb{F}_p$ (since 1 is sent to 1 the isomorphism fixes $\mathbb{F}_p$). Since $\mathbb{F}_{p^m}/\mathbb{F}_p$ is a Galois extension with Galois group $\mathbb{Z}/m\mathbb{Z}$, there are exactly m such isomorphisms.

In conclusion, $f(m, 6) = m$ if $m \mid 6$ and $f(m, 6) = 0$ otherwise.

(b) What is $f(6, n)$?

Solution: As above, we need only count injective homomorphisms from $\mathbb{F}_{p^6}$ to $\mathbb{F}_{p^n}$. If we have such a homomorphism $\mathbb{F}_{p^6}$ is isomorphic to its image. So $f(6, n)$ is 0 unless $\mathbb{F}_{p^n}$ has a subfield isomorphic to $\mathbb{F}_{p^6}$. We know that $\mathbb{F}_{p^n}$ has such a subfield if and only if $6 \mid n$, and in this case, there is a unique such subfield.

Suppose $6 \mid n$. We need only count isomorphisms from $\mathbb{F}_{p^6}$ to this unique subfield of $\mathbb{F}_{p^n}$ isomorphic to $\mathbb{F}_{p^6}$. Every such isormorphism can be identified with an automorphism of $\mathbb{F}_{p^6}$ fixing $\mathbb{F}_p$. As above, there are 6 such automorphisms.

So we see that $f(6, n) = 6$ if $6 \mid n$ and $f(6, n) = 0$ if $6 \nmid n$.

11. Prove that $\mathbb{Q}(\sqrt[3]{5})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.

Solution: We note that $\mathbb{Q}(\sqrt[3]{5})$ is not a Galois extension of $\mathbb{Q}$. The minimal polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}$ is $x^3 - 5$ (this polynomial is Eisenstein at $p = 5$). We see that $\mathbb{Q}(\sqrt[3]{5})$ contains one of these roots, but it does not contain the others: $\zeta_5^a \sqrt[3]{5})$ where $1 \leq a \leq 4$. We see this because $\mathbb{Q}(\sqrt[3]{5})$ is a subfield of $\mathbb{R}$, but these other roots are not real.

The cyclotomic field $\mathbb{Q}(\zeta_n)$ is an abelian extension of $\mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Subfields of abelian extensions are Galois since subgroups of abelian groups are automatically normal. Therefore, $\mathbb{Q}(\sqrt[3]{5})$ cannot be a subfield of $\mathbb{Q}(\zeta_n)$ for any n.